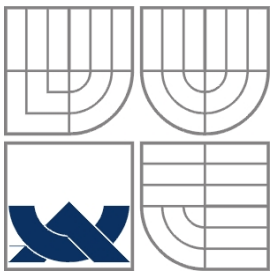
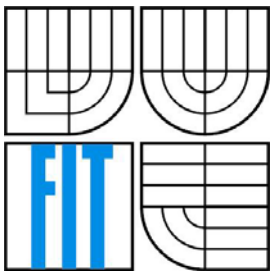


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

MAPOVÁNÍ BEZDRÁTOVÝCH TECHNOLOGIÍ V TERÉNU S VYUŽITÍM GPS

WIRELESS NETWORKS OUTDOOR MAPPING WITH GPS LOCALISATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. Petr Kabátek
AUTHOR

VEDOUCÍ PRÁCE — Ing. Pavel Očenášek
SUPERVISOR

BRNO 2007

Abstrakt

Úkolem mé práce je monitorovat v terénu bezdrátové technologie typu WIFI. Toto monitorování má probíhat tak, že budu procházet terénem a budu získávat informace o dostupných bezdrátových sítích WIFI. Mezi parametry těchto sítí patří například jméno sítě, síla signálu, typ zabezpečení atd.. Tyto parametry WIFI sítí budu zaznamenávat a ke každému takto vytvořenému záznamu přiřadím pomocí GPS přijímače informace o poloze ve které měření a získávání parametrů WIFI sítí proběhlo. Takto získané údaje (parametry + poloha) budou uloženy do databáze. Pomocí takto uložených dat v databázi potom bude možné provádět další složitější operace jako vytváření map bezdrátových sítí nebo zjišťování polohy přístupového bodu WIFI sítě atd..

Klíčová slova

wifi, gps, ssid, wep, wpa, wardriving, warchalking, warstroling, warboating, warflying, almanac, efemerida, mac, wgs-84, sjtsk

Abstract

This thesis deals with the monitoring of wireless nets in terrain. The author will be browsing terrain and there will be extracted some information about accessible wireless nets. For parameters of wireless nets we consider for example the name of wireless net, signal strength, type of security etc. These parameters (of wireless nets and position) are going to be recorded and saved into the database. Using this database it will be possible to perform some further operations like generation maps of wireless networks or detection positions of access points, etc..

Keywords

wifi, gps, ssid, wep, wpa, wardriving, warchalking, warstroling, warboating, warflying, almanac, efemerida, mac, wgs-84, sjtsk

Citace

Kabátek Petr: Mapování bezdrátových technologií v terénu s využitím GPS. Brno, 2007, diplomová práce, FIT VUT v Brně.

Mapování bezdrátových technologií v terénu s využitím GPS

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením Ing. Pavla Očenáška.
Další informace mi poskytli pan Ing. Martin Hrubý a paní Ing. Eliášová.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

……
Petr Kabátek
15.5. 2007

Poděkování

Poděkovat bych chtěl hlavně vedoucímu mé diplomové práce panu Ing. Pavlu Očenáškovi za poskytnutí rad a materiálů a také paní ing. Eliášové z Ministerstva práce a sociálních věcí za poskytnutí databáze územně identifikačního registru adres.

Obsah

1. Úvod

Stále více uživatelů sítě využívá přístup k Internetu a ostatním počítačům v domácnosti pomocí pohodlné a flexibilní domácí bezdrátové sítě. Přes mnohé výhody bezdrátového připojení existují také bezpečnostní rizika.

Nezabezpečíte-li bezdrátovou síť, otevřete dveře zvědavým sousedům a v horším případě útočníkům, kteří se zabývají nabouráváním do sítí - činností zvanou „wardriving“.

Warchalking, Wardriving, Warstroling, Warboating a Warflying to jsou pojmy, jimiž se hemží fóra, ve kterých se lze dozvědět spousta informací o mnoha NODECH po celé světě. Jsou to informace spojené především s bezdrátovými sítěmi (Internetem) v pásmu 2,4 GHz...

Warchalking

V roce 2002 vymyslel londýnský designer Matt Jones několik značek, kterými označují místa (budovy, chodníky, silnice, náměstí atd.) na nichž je možno naleznout bezdrátovou síť Wi-Fi. A Warchalking byl na světě. Brzy se ujal u mnoha nadšenců Wi-Fi sítí. Ti se posléze začali vzájemně informovat o přítomnosti "Wi-Fi" a to právě prostřednictvím symbolů navržených panem Jonesnem – obrázek č. 1. Když začal být internet veřejnou záležitostí, několik lidí se pokoušelo vytáčet náhodná telefonní čísla, aby zjistili jestli se na daném telefonním čísle nevyskytuje modem. Toto počínání, dnes bychom to mohli považovat za obdobu IP Scanu, se jmenovalo wardialing. [12] [13] [17]

Obrázek č. 1 :

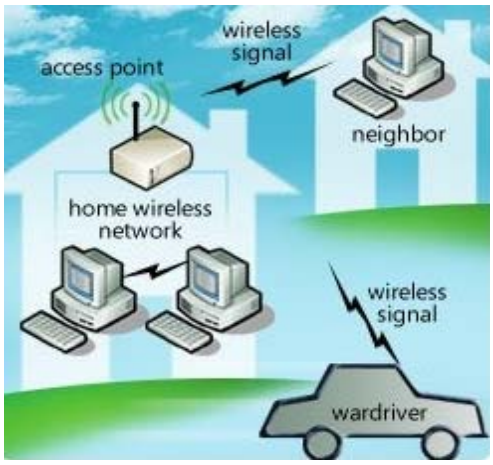
SSID otevřená SSID uzavřená Šifrovaná (WEP\WPA) síť

Tyto značky mohou být nakreslené například na chodník, silnici a jiná vhodná místa. Tyto značky jsou celosvětově známé, a tudíž jejich význam pochopí i Warchalker, pocházející z Japonska, při prohlídce Karlova mostu.

Další pojmy jako **Wardriving, Warstroling, Warboating a Warflying** jsou stejné jako **Warchalking –** obrázek č. 2**.** Liší se pouze v tom jakým způsobem provádíte monitorování bezdrátových sítí – při **Warchalkingu** chodíte pěšky s notebookem v ruce, kdežto například při **Wardrivingu** používáte k přemisťování automobil. U ostatních způsobů to platí obdobně – **Warboating –** loď, **Warflying** – letadlo a tak dále. V automobilu a podobných prostředcích s vámi samozřejmě musí ještě někdo spolupracovat – jeden řídí a druhý monitoruje a popřípadě ovládá antény – ty mohou být umístěny i na střeše vozu.

Příklad údajů viditelných u jednotlivých typů značek

OPEN NODE(otevřená síť) = otevřený přístup, je uvedeno SSID a rychlost (bandwidth)
CLOSED NODE(uzavřená síť) = uzavřený přístup, je opět uvedeno SSID
WEP NODE(šifrovaná síť) = přístup omezený WEP, je uvedeno SSID, adresa a rychlost



Obrázek č. 2 : Příklad wardriveringu

Warchalker je člověk pohybující se po městě s notebookem či PDA a chovající se "podezřele". Na svém počítači (PDA) používá některý ze speciálních softwarů určených k mapování bezdrátových sítí. Pokud se mu podaří zjisti některou z nezabezpečených sítí, pohotově poznamenává souřadnice(pokud je vybaven např. **GPS** přijímačem) či adresu a detaily pro připojení. Své informace poté poskytne přátelům či celému světu prostřednictvím internetu. **Warchalker** zároveň označuje zjištěné místo specielními značkami na zeď(chodník, …..) značky jsou uvedeny výše.

Nezapomíná přitom pochopitelně ani na obranu před snadným odhalením. Jméno svého počítače nastavil na něco vypadající dostatečně "legitimně", MAC adresu své síťové karty pokud možno průběžně mění a pochopitelně, je neustále v pohybu.

Legálnost warchalkingu

Samotný warchalking nelegálním podle všeho není ve Spojených Státech a podle všeho ani v České republice. Warchalking (**Wardriving, Warstroling, Warboating a Warflying**) je totiž pouze zjišťování volně dostupných informací aniž by síť byla jakkoliv využita či byly prováděny jakékoliv další aktivity na zjištěné síti. Nevyužívá tedy žádných dalších služeb ani prostředků sítě a neprovádí tím pádem ani žádné přenosy dat ani změny dat - jediné co je ze sítě využito je služba dotazu na parametry a existenci sítě.

Warchalking je ostatně možný i s použitím pomůcek dodaných přímo výrobcem síťové karty (či operačního systému) - základní zjištění dostupných sítí i jejich parametrů je totiž zpravidla zabudováno i v podpůrných programech. [12] [13] [17]

Vysvětlení pojmů jako GPS, WEP, WPA, bezpečnost bezdrátových sítí, šifrování, a další budou vysvětleny v následujících kapitolách zabývajících se technologiemi GPS a WI-FI.

2. GPS (Global Positioning System)

2.1 Úvod

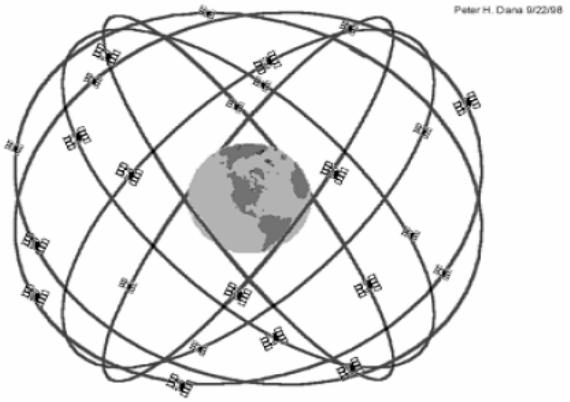
Lidstvo se odpradávna snažilo vyřešit problém s navigací. Dlouho nezbývalo než se spoléhat na přírodu a orientovat se pomocí výrazných bodů v terénu. Hůře na tom byli námořníci, neboť těžko mohli považovat pár nahodilých ostrůvků za výrazné body v terénu, a tak se museli spoléhat na hvězdnou oblohu a na jednoho ze členů posádky, který za pomoci sextantu dokázal přesně určit polohu, kde se loď právě nacházela. Na začátku dvacátého století začaly při navigaci pomáhat rádiové signály. Tento způsob navigace obrovsky zpopularizovaly obě světové války. A původně pro vojenské účely vznikl koncem sedmdesátých let dvacátého století i navigační systém GPS (Global Positioning System).

Systém GPS využívá služeb 27 družic (z tohoto počtu jsou tři záložní), které jsou rozmístěny na šesti drahách ve výšce více než dvacet tisíc kilometrů. Každý z těchto satelitů vysílá signál, který GPS přijímač dokáže přijmout a přesným změřením času, za který signál dorazil ze satelitu do přijímače, umí přístroj vypočítat svoji vzdálenost od satelitu. Aby pak přijímač dokázal vypočítat i svoji polohu, potřebuje takto vyhodnotit signál alespoň ze tří družic. Toho se docílí takovým uspořádáním družic, aby z kteréhokoli místa na zemi byly vidět minimálně čtyři družice. Pro správné změření času jsou jak družice, tak přístroje vybaveny velmi přesnými atomovými hodinami. Kromě vzdálenosti mezi přístrojem a družicemi je také potřeba znát polohu jednotlivých družic, a proto informace o své poloze družice neustále vysílají. A protože signál vysílaný z družic je velmi slabý, je poslední podmínkou správného fungování systému ještě to, aby byla zaručena přímá viditelnost přístroje na otevřenou oblohu.

Do 1.května roku 2000 byla přesná poloha zatížena chybou – tato chyba byla generována automaticky a uměle americkou armádou, která se obávala toho, že by relativně přesný poziční systém zneužili teroristé a mohli by tak přesně zaměřit některé strategické cíle v USA. Přesnou polohu uměli urči pouze vojenské navigační přístroje, které uměli tuto chybu odstranit. Nakonec se však ukázalo, že armáda nemá dostatek těchto přístrojů a pro teroristy není problém si tyto přístroje opatřit, takže 1.května 2000 byla tato umělá chyba armádou zrušena. [1]

2.2 Jak funguje GPS?

Systém GPS aktivně využívá celkem 24 satelitů, které se pohybují po šesti orbitách ve 12 hodinových periodách – obrázek č. 3. Po každé orbitě se tedy pohybují celkem čtyři satelity. Toto rozložení satelitů pak pokrývá celý povrch zeměkoule a lze tedy určit polohu na jakémkoli „otevřeném“ místě země.

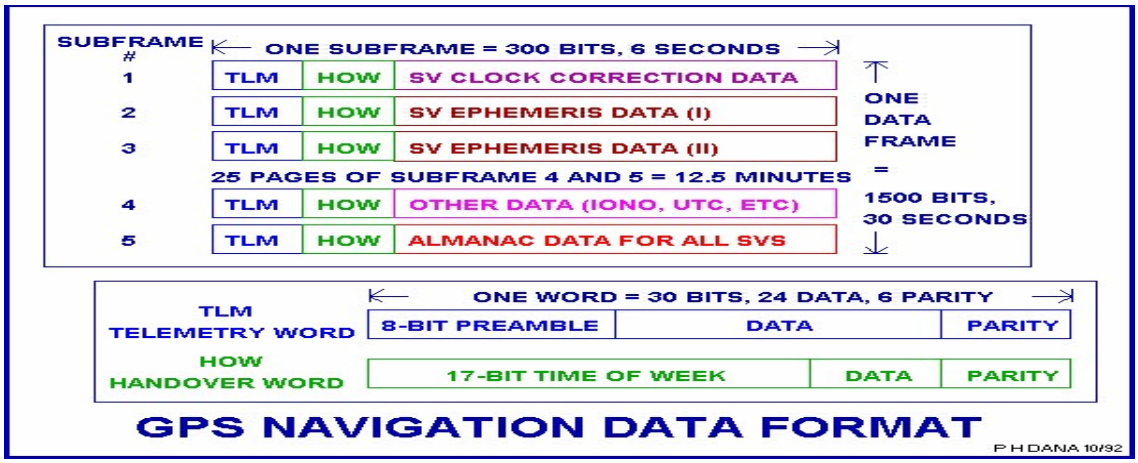


Obrázek č. 3 : Satelity GPS na orbitách

Orbity se od sebe vzájemně odklání o 60 stupňů. Satelity se pohybují po orbitách ve výšce 20 200 km nad povrchem země. Z jednoho místa na Zemi bývá v přímé viditelnosti antény přijímače 6 až 12 družic. Na palubě družic NAVSTAR jsou 3 až 4 velmi přesné atomové hodiny (nezbytné pro funkci systému), s cesiovým a rubidiovým oscilátorem, a dále pak detektory, kontrolující dodržování zákazu zkoušek nukleárních zbraní.Systém GPS je založen na zpoždění rádiového signálu který každý satelit vysílá. GPS využívá několik specifických frekvencí označených L1 až L5. Frekvence jsou voleny záměrně tak, aby odolávali některým meteorologickým vlivům.

„L1“ (1575,42 MHz), kde je vysílán C/A kód je dostupná pro civilní uživatele systému GPS.
„L2“ (1227,62 MHz), kde je šířen vojenský P/Y kód, který je šifrovaný, je přístupná pouze pro tzv. autorizované uživatele (např. vojenské služby USA).
„L3“ (1381,05 MHz) obsahuje signály, které souvisí s další funkcí systému GPS, odhalováním startů balistických raket (čímž doplňuje satelity náležící k Defense Support Program), jaderných výbuchů a dalších vysokoenergetických zdrojů v infračerveného záření.
„L4“ (1841,40 MHz) se využívá pro měření ionosferického zpoždění. Průchod signálu ionosférou způsobuje totiž přidání dodatečného zpoždění ke zpoždění způsobenému vzdáleností, které se promítne do chyby polohy. Toto ionosférické zpoždění lze eliminovat, jestliže měříme zpoždění na dvou kmitočtech.
„L5“ (1176,45 MHz) se plánuje jako civilní safety-of-life (SoL) signál. Tato frekvence spadá do mezinárodně chráněné oblasti letecké navigace, ve které je malé nebo žádné rušení za všech podmínek. S vypuštěním prvního Block IIF satelitu, který bude poskytovat tento signál se počítá na rok 2007.

Běžné přijímače pracují pouze na kanálu L1. Druhý kanál L2 se používá současně s L1 pro velmi přesná měření. Všechny satelity jsou synchronizovány tak, že vysílají data ve stejný okamžik. Každá družice vysílá tok binárních dat, která jsou dělena do slov o 30 bitech. Pouze 24 bitů je informačních. Zbylých 6 bitů je použito pro zabezpečení a to Hammingovým kódem (32,26) se vzdáleností 4. Každé vyslané slovo má tedy 30 bitů – obrázek č. 4. Deset slov tvoří podrámec a pět podrámců tvoří rámec. Takže celý rámec má celkem 1500 bitů. Jeden bit trvá 20 ms a celý rámec tedy trvá 30 s. První, druhý a třetí podrámec obsahuje aktuální informace o stavu družice – tato informace se aktualizuje několikrát za den. Mezi aktualizacemi je tato informace konstantní. Čtvrtý a pátý podrámec obsahuje informace o celém systému GPS a jejich obsah se aktualizuje několikrát za týden. Mezi okamžiky aktualizace se obsah podrámců pravidelně opakuje s periodou 25 rámců. Celá informace o systému GPS je tedy obsažena v posloupnosti 5 * 25 = 125 podrámců. Této posloupnosti říkáme navigační zpráva. Podrámec daného čísla (1 až 5) má 25 možných významů, kterým říkáme stránka a označujeme je pořadovým číslem rámce ve zprávě. První stránka od začátku zprávy má číslo 1. Každý satelit vysílá data rychlostí 50 Hz. [7]



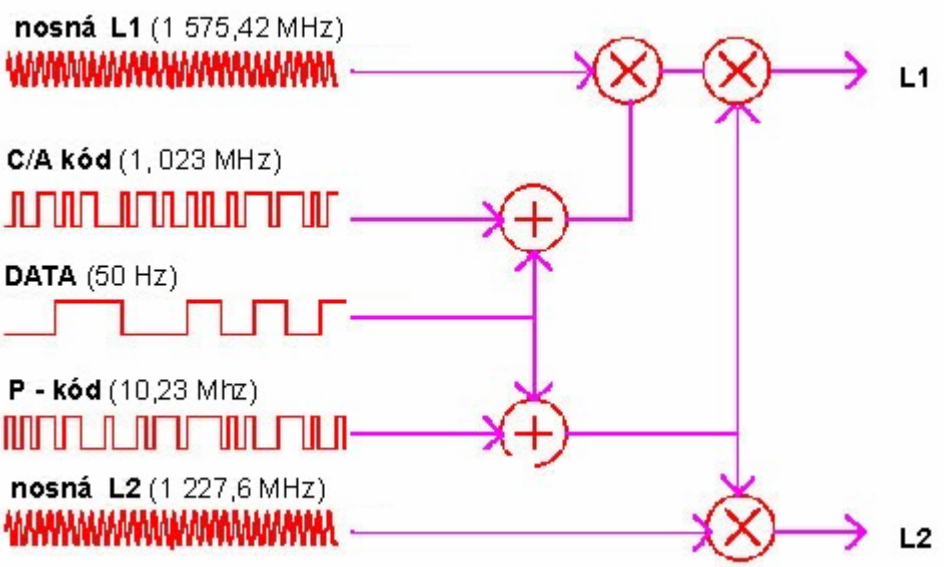
Obrázek č. 4 : Datový formát komunikace GPS

Dále každý satelit posílá zprávu o své poloze vyjádřenou tzv. efemeridou, což je astronomické přesné určení polohy kosmického tělesa v určitém čase, přesný údaj o čase, dále odhad zpoždění signálu v ionosféře a ještě celou řadu dalších údajů. Mimoto vysílají satelity tzv. almanac, což je vlastně databáze dalších satelitních stanic. Tuto databázi si přijímač GPS uloží do paměti ihned po přihlášení a dále si ji aktualizuje. V databázi jsou uloženy kódy okolních satelitů a i jejich přibližná poloha, z níž si přijímač umí odhadnout, kdy se zhruba mohou objevit na horizontu.

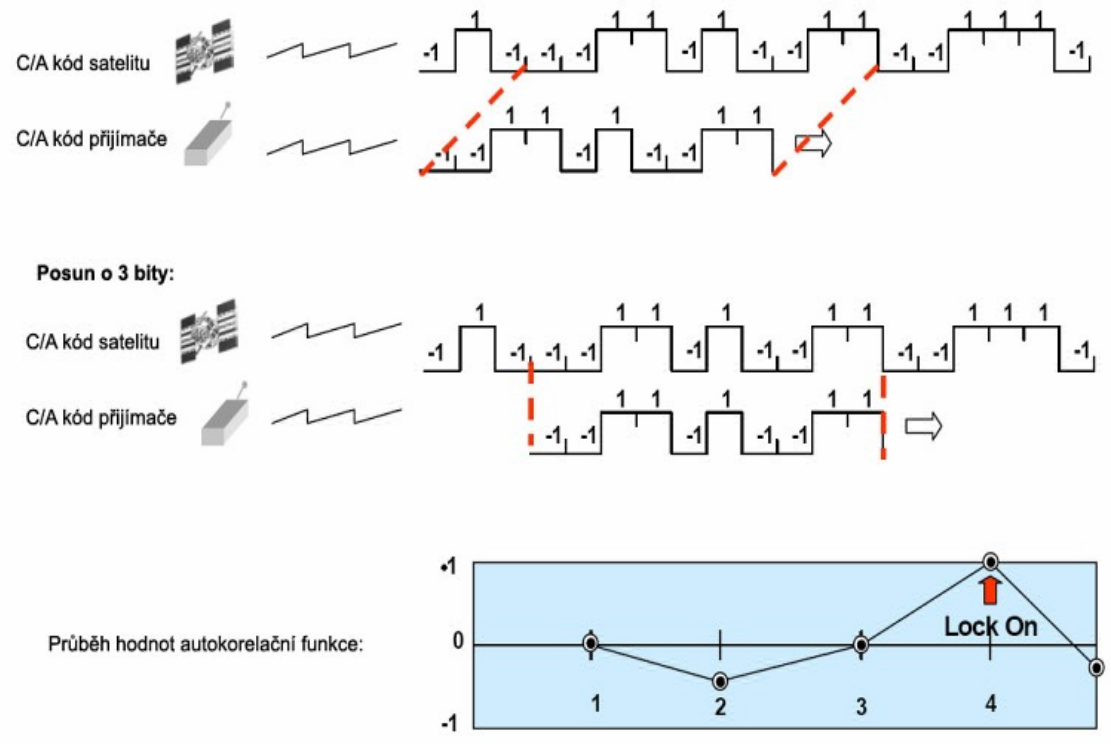
Pro přenos bitového toku se používá modulace BPSK (binary phase shift keying), - podle hodnoty bitu se fáze nosné mění o 180 stupňů. Protože všechny satelity vysílají ve stejný okamžik a na stejné frekvenci je nutné nějak rozpoznat jednotlivé satelity – proto je před odesláním každá posloupnost vynásobena pseudonáhodnou posloupností +1 a -1. Této posloupnosti říkáme PN kód (v anglicky psané literatuře Pseudo Random Noise Code). Takto násobená posloupnost potom vypadá jako náhodný šum – obrázek č. 5. Každý satelit má samozřejmě tento pseudonáhodný kód jiný – podle toho je potom satelit u pozemních přijímačů rozpoznán.

V přijímači se opět provede vynásobení přijatého signálu pseudonáhodným kódem a to způsobí to, že se úplně obnoví původní informace ze satelitu – ostatní signály z nepotřebných satelitů jsou potlačeny jako šum. [7]

Obrázky znázorňující funkci satelitů a přijímačů



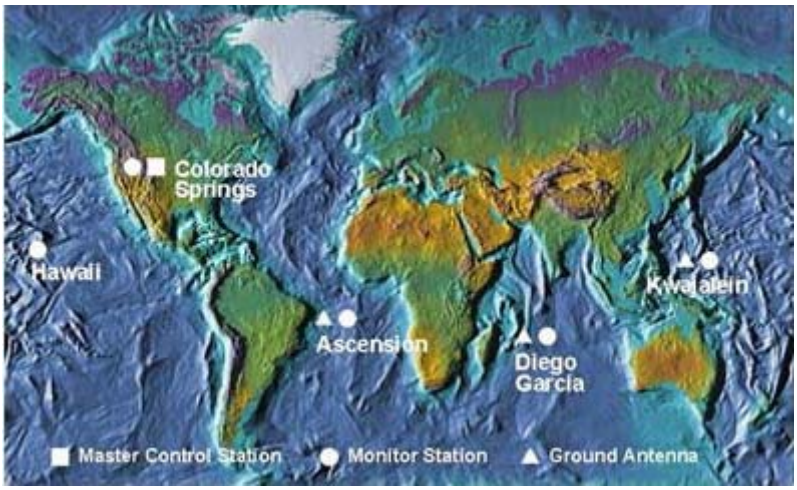
Obrázek č. 5 : Znázorňuje vznik signálu GPS



Obrázek č. 6 : Znázorňující synchronizaci satelitu a přijímače GPS

Řídící a kontrolní střediska systému GPS

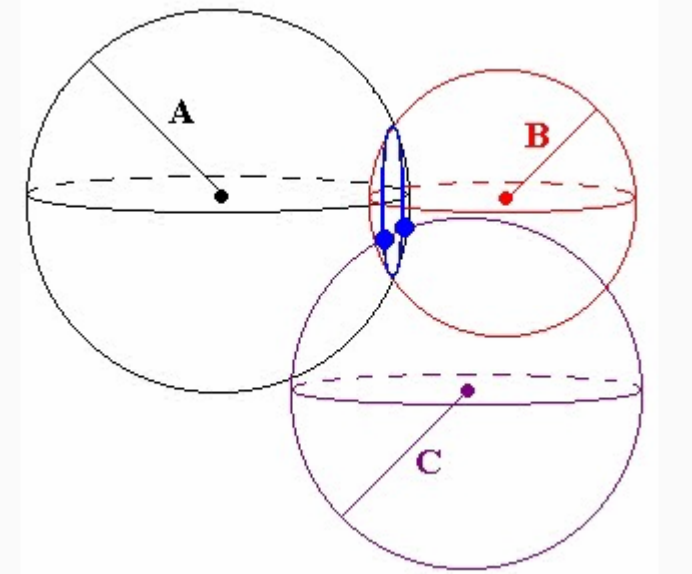
Systém GPS je řízen z ústředí Navstar Headquarters na letecké základně (AFB) Los Angeles v Californii v USA. Hlavní pozemní stanice se nachází na letecké základně Falcon v Coloradu a hlavní operační řídicí středisko na letecké základně Schriever v Coloradu, které provozuje letectvo Spojených států amerických (USAF), 2nd Space Operations Sq. Po světě je rozmístěno 5 dalších monitorovacích stanic (Havajské ostrovy, Kwajalein, Diego Garcia, Ascension, Colorado Springs) a 3 povelové stanice (Kwajalein, Diego Garcia, Ascension) – Obrázek č. 7. [2]



Obrázek č. 7 : Kontrolní a řídicí centra GPS

2.3 Určení polohy GPS

Samotné určení polohy je založené na principu takzvané trilaterace – Obrázek č. 8. K měření vzdálenosti využívá trilaterace zpoždění signálu vyslaného od satelitu. Přijímač si takto zjistí vzdálenost od několika satelitů(minimálně 3 až 4 satelity) a na základě toho potom přijímač vypočte svou polohu.



Obrázek č. 8 : Trilaterace

Výpočet polohy funguje tak, že přijímač postupně zná vzdálenost k jednomu satelitu – tedy přijímač ví, že leží někde na povrchu koule o poloměru získané vzdálenosti se středem ve zkoumaném satelitu. Pokud přijímač zjistí vzdálenost k dalšímu satelitu(získá tedy údaj o další „kouli"), pak může přijímač provést průnik dvou povrchů těchto koulí a tím získá kružnici(elipsu) na které se nachází přijímač. Pokud poté přijímač získá vzdálenost k dalšímu satelitu – tedy má k dispozici další „kouli", potom může provést průnik povrchu této koule s dříve získanou kružnicí(elipsou) a získá tím dva body. Z těchto dvou bodů bude ležet jeden buď hluboko pod povrchem nebo vysoko nad povrchem země – tento bod polohu určitě neznačí. Druhý bod značí „přesnou" polohu přijímače. Tento princip se nazývá trilaterace – lépe je vidět na obrázku č. 8.

K určení opravdu „přesné" polohy je zapotřebí aby hodiny satelitů a hodiny přijímače byly zcela synchronní. Pokud by se totiž lišili jen o vteřinu nebo i míň, docházelo by k obrovským chybám. Proto k určení „přesné" polohy je potřeba 4 družic, kdy časová odchylka je jednou z hledaných neznámých. Další hledané neznámé jsou jednotlivé složky pozice – *x, y, z*. Tedy 4 neznámé, 4 rovnice a pro určení „přesné" 3D pozice 4 satelity.

Pokud jsou k dispozic pouze 3 satelity počítá se pouze 2D pozice, která není přesná. Přijímače při příjmu signálů tří družic tedy předpokládají, že jsou na povrchu Země a určí tři neznámé (zeměpisná šířka, délka a odchylka hodin). [8]

2.4 Chyby při určování polohy

Při určení polohy se nejprve změří vzdálenost ke družicím, dále se vypočtou polohy družic a nakonec je vypočítána poloha přijímače. Z tohoto postupu určování polohy vyplývá, že k chybě může dojít :

- Při měření vzdálenosti k satelitům
- Při výpočtu polohy satelitů
- Při počítání polohy přijímačem

2.4.1: Chyba při měření vzdálenosti satelitu od přijímače

Signál vysílaný satelitem prochází atmosférou a ta je zdrojem atmosférického šumu. To jak velká odchylka při průchodu atmosférou vznikne záleží na kmitočtu vysílaného signálu. Například pro kmitočet L1 (1575,42 MHz) je odchylka až 7,5 m. Pro kmitočet L2 (1227,62 MHz – vojenský sektor) je odchylka až 1,5 m. Další zdroj chyb tvoří nepřesná znalost rychlosti šíření signálu v jednotlivých vrstvách atmosféry – původně se totiž předpokládalo, že se signál šíří atmosférou rychlostí světla – z fyziky je ale známo, že takovouto rychlostí se toto vlnění šíří pouze ve vakuu. Při průchodu atmosférou se tedy signál šíří menší rychlostí než je rychlost světla. Pro civilní sektor může chyba dosahovat 5 až 10 metrů, u vojenského sektoru je mnohem menší a dá se dokonce i eliminovat – a to měřením na dvou kmitočtech.

Jednotlivé části atmosféry, které nejvíce ovlivňují signál – troposféra, ionosféra. Nejvíce způsobuje chybu průchod signálu ionosférou – nejvíce záleží na jejím stavu – ovlivněn například ročním obdobím, polohou slunce atd..

2.4.2: Chyba při výpočtu polohy satelitů

Algoritmus výpočtu polohy družice je popsaný v definici GPS. Vstupem tohoto algoritmu jsou parametry dráhy družice, které jsou v signálu vysílaném družicí. Těmto parametrům říkáme efemeridy. Efemeridy zjišťují pozemní stanice systému GPS, které sledují družice a z jejich pohybu předpovídají efemeridy, které pak odesílají na družici a ta je zařazuje do svého vysílání. Jsou proto možné dva typy chyb - chyba v predikci efemerid a chyba pohybu družice (např. v důsledku nárazu meteoritu). Směrodatná odchylka chyby vzdálenosti v důsledku chyby polohy družice je přibližně 4 m a je přirozeně stejná pro civilní i vojenský sektor.

2.4.3: Chyba při výpočtu vlastní polohy přijímačem

Chyba u vlastního výpočtu je vlastně dána těmi předchozími. Efektivní chyba při vlastním výpočtu je dána součinem odchylky při výpočtu vzdálenosti a koeficientu, který charakterizuje rozmístění družic na hemisféře (tento koeficient se nazývá *DOP* - dilution of precision, rozptyl přesnosti). Pro horizontální chybu je to obdobný součin odchylky vzdálenosti a koeficientu *HDOP*. A pro vertikální chybu se koeficient značí *VDOP*. Pro Českou Republiku nabývají hodnoty koeficientu zhruba hodnot - *DOP* = 1,87, přičemž *VDOP* = 1,55 a *HDOP* = 1,05. [9] [14] [15]

2.5 Komunikační protokol NMEA

(**Přesný komunikační protokol lze získat pouze od asociace NMEA a to za určitý peněžitý obnos. A i potom nesmí být dále šířen. Proto zde uvedu pouze informace, které jsou volně dostupné na internetu. Proto také nemohu přesně říci jestli jsou tyto údaje aktuální a přesné.**)

NMEA 0183 – je komunikační protokol technologie GPS, který používají satelity a pozemní GPS přijímače pro komunikaci.

Civilní pozemní přijímače se většinou dají připojit k počítači. Ať už se jedná o bezdrátové přijímače(Bluetooth), drátové(USB, RS232) vždy komunikují s počítačem na úrovni sériového rozhraní RS232. Proto se nastavují parametry komunikace – a to přenosová rychlost – 4800 baudů, počet datových bitů – 8 bitů, přičemž sedmý bit (MSB) je vždy nulový, počet stop bitů – 1 bit nebo více a parita není žádná. Toto nastavení platí pro většinu přijímačů.

Veškerá data jsou posílána ve formě vět. Věta může obsahovat pouze ASCII znaky a znaky konce řádku - *<CR>* a *<LF>* (*0x0d*, *0x0a*). Každá věta začíná znakem $ (dolar) a končí sekvencí *<CR><LF>*.

Existují tři základní druhy vět:

- **věty ze strany mluvčího (talker sentences)**
- **proprietární věty (proprietary sentences)**
- **dotazovací věty (query sentences)**

2.5.1: Obecný formát věty ze strany mluvčího

$ttsss,d1,d2,....<CR><LF>

Věta tedy začíná znakem „$“ a končí znakem konce řádku *<CR><LF>*. První dva znaky „tt“ po znaku dolar označují mluvčího (talker identifier). Další tři znaky „sss“ jsou identifikátor věty (sentence identifier). Dalšími položkami položkami ve větě jsou datové složky *„d1“, „d2“ ..... „dN“* oddělené čárkami. Po datových složkách následuje kontrolní součet a potom zakončení věty znakem konce řádku. Pokud zrovna není některá datová položka k dispozici je pozice pro danou položku prázdná oddělená čárkami – *d1,,d3,d4* – z příkladu je vidět, že datová položka *d2* nebyla k dispozici.

Kontrolní součet začíná znakem hvězdička ("*") a za ní jsou dvě hexadecimální číslice představující logickou operaci XOR (exclusive OR) ze všech znaků mezi "$" a "*". Samotný dolar a hvězdička se do kontrolního součtu nezapočítávají. Každá věta může obsahovat nejvýše 80 znaků plus "$" a *<CR><LF>*, celkem tedy 83 bajtů.

2.5.2: Proprietární věty

Věty proprietární umožňují výrobcům nadefinovat vlastní větu. Tyto věty začínají sekvencí "$P", pak následuje třípísmenný identifikátor výrobce, a dále následují jednotlivé datové položky v souladu s přáním výrobce. Obecný formát věty musí být zachován. [9] [14] [15]

2.5.3: Dotazovací věty (query sentences)

Pomocí dotazovacích vět může posluchač(přijímač) požádat mluvčího(satelit) o zaslání konkrétní věty. Obecný formát dotazovací věty je :

$ttllQ,sss<CR><LF>

Věta zase začíná znakem dolar a končí znakem konce řádku. První dva znaky za dolarem „tt“ identifikují přijímač, který žádá o daný typ věty. Další dva znaky „ll“ označují toho, komu je žádost zasílána – tedy některý ze satelitů. Pátý znak „Q“ označuje že se jedná o dotazovací větu – Q – question. Následující tři znaky „sss“ označují o jaký druh věty se žádá - sentence identifier. Příklad dotazovacího příkazu - *$CCGPQ,GGA<CR><LF>* - v tomto příkazu žádá počítač „CC“ GPS přijímač „GP“ o zasílání věty typu „GGA“ .

Dvoupísmených identifikátorů existuje několik – např. GPS přijímač se značí „GP“, počítač se značí „CC“ ... Typů vět je také několik, ale běžné civilní GPS přijímače používají pouze čtyři typy : GSA, RMC, GSV, GGA. [9] [14] [15]

GSA, aktivní satelity a DOP (Dilution Of Precision)

Příklad : *$GPGSA,A,3,29,26,22,09,07,05,04,,,,,1.7,1.0,1.4*30*

#	formát	příklad	komentář
1	c	A	Přepínání mezi N-rozměrnými módy (A=automatické, M=manuální)
2	d	3	Počet dimenzí N (1=?, 2=2D, 3=3D)
3	dd	29	ID prvního satelitu použitelného pro výpočet
4	dd	26	ID druhého satelitu použitelného pro výpočet
5	dd	22	ID třetího satelitu použitelného pro výpočet
6	dd	09	ID čtvrtého satelitu použitelného pro výpočet
7	dd	07	ID pátého satelitu použitelného pro výpočet
8	dd	05	ID šestého satelitu použitelného pro výpočet
9	dd	04	ID sedmého satelitu použitelného pro výpočet
10	dd	N.A.	ID osmého satelitu použitelného pro výpočet
11	dd	N.A.	ID devátého satelitu použitelného pro výpočet
12	dd	N.A.	ID desátého satelitu použitelného pro výpočet
13	dd	N.A.	ID jedenáctého satelitu použitelného pro výpočet
14	dd	N.A.	ID dvanáctého satelitu použitelného pro výpočet
15	d.d	1.7	PDOP (Position Dilution Of Precision) v metrech
16	d.d	1.0	HDOP (Horizontal Dilution Of Precision) v metrech
17	d.d	1.4	VDOP (Vertical Dilution Of Precision) v metrech
18	*xx	30	Kontrolní součet

Tabulka č. 1

RMC (Recommended Minimum Navigation Information) Minimální doporučená informace pro navigaci

Příklad : *$GPRMC,170138.615,A,4912.2525,N,01635.0378,E,0.04,16.43,280705,,*32*

#	formát	příklad	komentář
1	hhmmss.sss	170138.615	Čas (UTC)
2	c	A	Status (A=OK, V=varování)
3	ddmm.mmmm	4912.2525	Zeměpisná šířka
4	c	N	Indikátor sever/jih (N=sever, S=jih)
5	ddmm.mmmm	01635.0378	Zeměpisná délka
6	c	E	Indikátor východ/západ (E=východ, W=západ)
7	d.d	0.04	Vodorovná rychlost (Speed Over Ground, v uzlech)
8	d.d	16.43	Kurz pohybu ve stupních
9	ddmmyy	280705	Datum ddmmyy
10	d.d	N.A.	Magnetická deklinace ve stupních
11	c	N.A.	Indikátor východ/západ (E=východ, W=západ)
12	*xx	32	Kontrolní součet

Tabulka č. 2

GSV (Satellites in View) Informace o družicích

Množství údajů závisí na počtu viditelných družic. Jedna věta může obsahovat nejvýše 80 znaků, což vystačí pouze k uložení dat týkajících se nejvýše čtyř družic. Informace proto bývá rozdělena do několika dílčích vět. [9] [14] [15]

Příklad : *$GPGSV,3,1,11,09,84,297,41,05,48,256,45,07,38,059,41,26,22,178,41*74*
*$GPGSV,3,2,11,24,13,063,00,14,12,324,00,30,12,251,00,22,12,286,38*78*
*$GPGSV,3,3,11,29,10,173,35,04,09,105,30,18,06,254,00*46*

#	formát	příklad	komentář
1	d	3	Celkový počet vět (číslují se od 1)
2	d	1	Číslo aktuální věty (taktéž se čísluje od 1)
3	dd	11	Počet viditelných družic
4	dd	09	Identifikační číslo družice
5	dd	84	Úhlová výška, kde se daná družice nachází
6	ddd	297	Azimut, kde se daná družice nachází
7	dd	41	Odstup signálu od šumu (SNR - Signal to Noise Ratio). Je-li tento údaj roven nule, nelze daný satelit využít k výpočtu polohy. Nejčastěji proto, že je zastíněn.
...	...	...	Podle počtu viditelných družic mohou následovat další čtveřice údajů (4-7)
n	*xx	74	Kontrolní součet

Tabulka č. 3

GGA – zeměpisná délka a šířka, geodetická výška, čas určení souřadnic

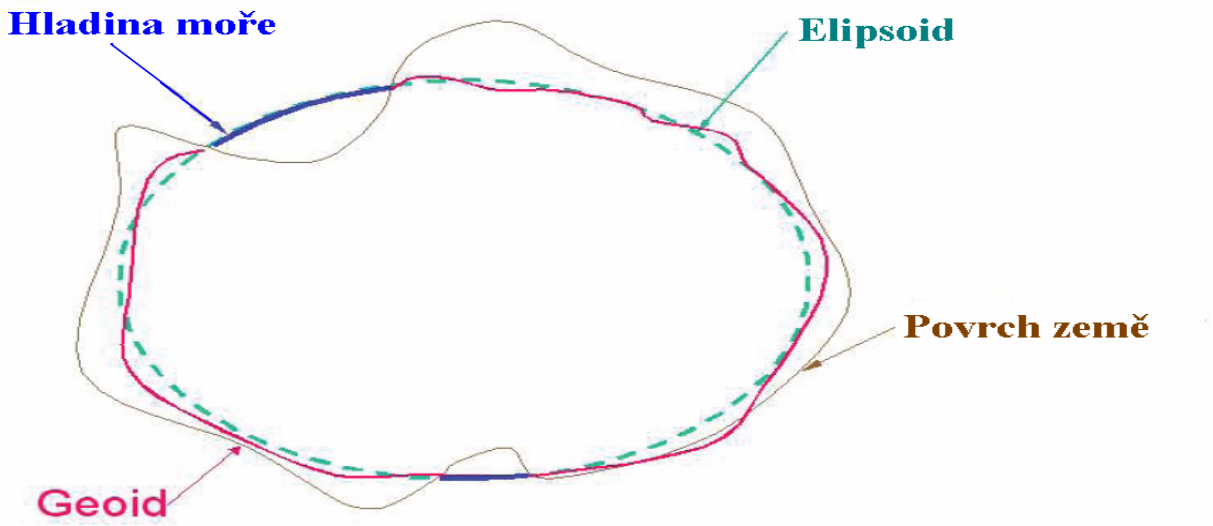
Příklad : *$GPGGA,170139.615,4912.2526,N,01635.0378,E,1,07,1.0,357.5,M,43.5,M,0.0,0000*7D*

#	formát	příklad	komentář
1	hhmmss.sss	170139.615	Čas (UTC), pro který platí údaje o vypočtené pozici
2	ddmm.mmmm	4912.2526	Zeměpisná šířka
3	c	N	Indikátor severní/jižní šířka (N=sever, S=jih)
4	dddmm.mmmm	01635.0378	Zeměpisná délka
5	c	E	Indikátor východní/západní délky (E=východ, W=západ)
6	d	1	Indikátor kvality: 0 — nebylo možno určit pozici 1 — pozice úspěšně určena 2 — pozice úspěšně určena (diferenční GPS)
7	dd	07	Počet viditelných satelitů 00 — 12
8	d.d	1.0	Vliv rozestavění družic na určení polohy HDOP (*Horizontal Dilution of precision*)
9	d.d	357.5	Výška antény nad elipsoidem
10	c	M	Jednotka pro předchozí údaj (č.9) (M=metr)
11	d.d	43.5	Geoidal separation, rozdíl mezi WGS-84 zemským elipsoidem a střední úrovní moře (geoid). Znaménko mínus znamená, že střední úroveň země je pod elipsoidem.
12	c	M	Jednotka vzdálenosti pro předchozí položku (č.11) (M=metr)
13	d.d	0.0	Stáří poslední aktualizace DGPS. Údaj je uváděn v sekundách. Jestliže údaj chybí, nepoužívá se DGPS.
14	dddd	0000	Identifikační číslo referenční stanice pro DGPS (0000 — 1023)
15	*xx	7D	Kontrolní součet

Tabulka č. 4

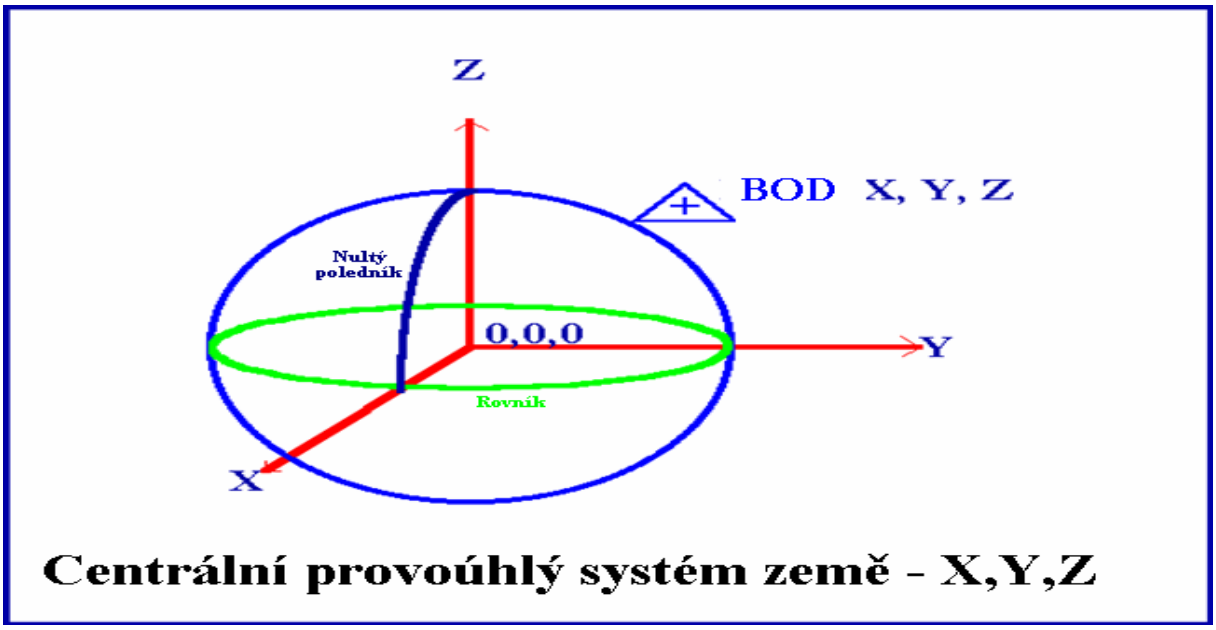
2.6 Souřadné systémy technologie GPS

Jednotlivé satelity vysílají informace o své poloze ve formě souřadnic, které jsou vztažené k souřadnicovému systému ECEF WGS-84 (Earth Centered Earth Fixed, World Geodetic System 1984). Jedná se o pravoúhlý systém(obrázek č.10) s počátkem souřadnic ve středu referenčního elipsoidu – obrázek 9, který představuje naši Zemi.



Obrázek č. 9 : Referenční Elipsoid

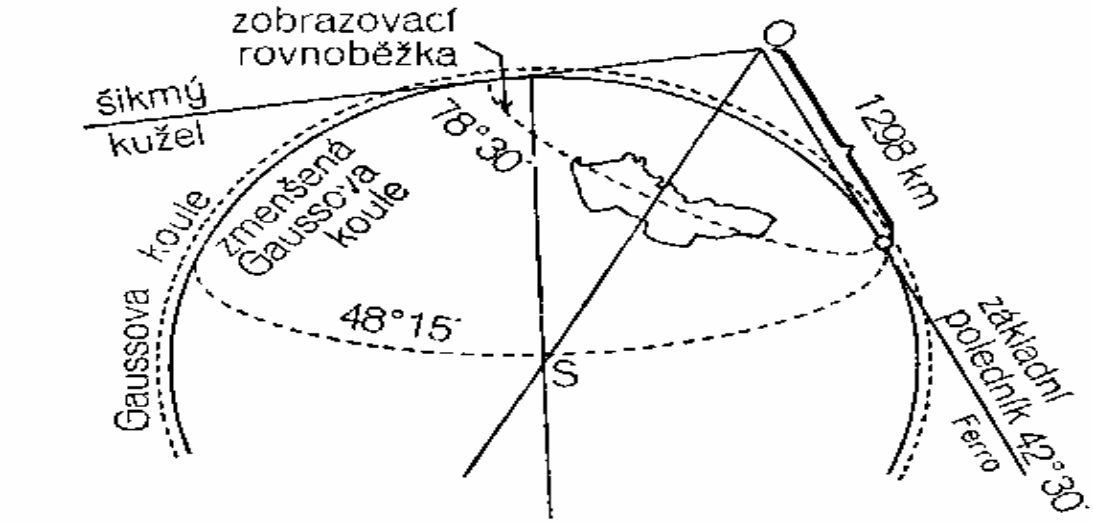
U ECEF WGS-84 (Earth Centered Earth Fixed, World Geodetic System 1984) je maximální odchylka geoidu od Země 60 metrů. Geoid se špatně matematicky popisuje. Proto se jako referenční model používá elipsoid – lépe je to vidět na obrázku č. 9,10 – s tímto elipsoidem se už dá počítat. Do geometrického středu tohoto elipsoidu je umístěn počátek souřadné soustavy — bod [0,0,0]. Osa z je totožná s osou rotace, osa x prochází průsečíkem rovníku a Greenwichského poledníku (nultého). Osa y je zvolena tak, aby systém x, y, z byl pravotočivý.



Obrázek č. 10 : Pravoúhlý souřadný systém

Všechny výpočty jsou tedy založeny na tomto souřadnicovém systému. Jakmile jsou výpočty dokončeny jsou souřadnice převedeny na běžné zeměpisné souřadnice (zeměpisná délka a šířka). Třetí souřadnicí je výška nad referenčním elipsoidem. Tady potom nastává problém a to v tom, že souřadný systém zeměpisné šířky, délky a výšky nad elipsoidem není pravoúhlý a uživatel s těmito hodnotami nemůže počítat – například vzdálenosti dvou různých bodů. Proto je nutné pro možnost pracování převést tyto hodnoty do jiného souřadnicového systému – samozřejmě pravoúhlého.

Tyto pravoúhlé souřadné systémy jsou většinou omezeny na menší území – například pro Českou Republiku byl vytvořen pravoúhlý souřadný systém S-JTSK – obrázek č. 11.



Obrázek č. 11 : Souřadný systém S-JTSK

Při převodu ze souřadnic zeměpisné šířky, délky a výšky na pravoúhlý systém S-JTSK jsou vypočteny pravoúhlé souřadnice *X* souřadnice *Y*. S těmito pravoúhlými souřadnicemi už se dají počítat vzdálenosti dvou naměřených bodů. S těmito souřadnicemi budu také pracovat ve svém projektu.

Přepočet souřadnic z jednoho systému do druhého je velice složité a je založeno na velkém množství konstant, které zde vypisovat nebudu – na internetu lze nalézt různé návody pro tyto převody – algoritmy pro přepočet těchto souřadných systémů budou uvedeny v jedné z kapitol implementace.

3. Bezdrátová technologie WI-FI

3.1 Úvod

Technologie WLAN se zrodila v roce 1992, kdy bylo shodně americkým FCC a evropským ETSI uvolněno bezlicenční radiové pásmo ISM 2,4 GHz. V něm pracují i další zařízení, z nichž nejzajímavější jsou asi zařízení bluetooth (pro která později vznikla samostatná norma 802.15), mikrovlnné trouby a americké bezdrátové telefony. Od té doby prošly velkým vývojem, byly standardizovány a stali se součástí většiny hlavně menších firem a domácností. Během tohoto vývoje vzniklo několik standardů a další se připravují.

O výklad a správu jednotlivých standardů se stará certifikační autorita WECA, která také testuje schopnost WiFi zařízení jednotlivých výrobců mezi sebou vzájemně spolupracovat. Tato aliance byla přejmenována v roce 2003 na WiFi Alliance (WiFi = Wireless Fidelity). Příčinou vzniku této organizace byly problémy s prvními sériemi výrobků pracujícími dle standardu 802.11b, kdy mezi sebou často nebylo možné jednotlivé výrobce a výrobky kombinovat. To samozřejmě vedlo k nedůvěře uživatelů a k jejich nezájmu o bezdrátové sítě. WiFi Alliance tedy zkoumá jestli dané wifi zařízení bude schopné spolupracovat s ostatními zařízeními a udělí mu certifikační značku – je vidět na obrázku 12.

Obrázek č.12 : Certifikační značka

V roce 1997 došlo ke vzniku první normy – 802.11, která specifikovala standard bezdrátové sítě v pásmu ISM a nabízela rychlosti 1 a 2 Mb/s. Protože tento standard nabízel pouze takto malé přenosové rychlosti v době kdy už bez problémů funguje 100 Mbit Ethernet, tak dochází v roce 1999 k vytvoření dvou nových standardů. Nejdříve byl uveden standard 802.11b a o něco později standard 802.11a. Standard „b“ dovoloval teoretickou rychlost 11 Mbit za sekundu v pásmu 2,4 GHz a standard „a“ dovoloval teoretickou rychlost až 54 Mbit za sekundu. U těchto standardů ale nebyla řešena bezpečnost přenosu. Před tím než byl ustanoven standard 802.11i zabývající se výhradně bezpečností bezdrátových sítí v roce 2004 vznikl ještě jeden standard 802.11g který byl zpětně kompatibilní se standardem „b“ a zvětšoval teoretickou rychlost až na 54 Mbit za sekundu v pásmu 2.4 GHz. Standard „g“ vznikl roku 2003. V roce 2003 byl také přijat další standard a to 802.11f, který zavedl pravidla pro bezproblémový roaming. V roce 2004 byla vytvořena také norma 802.11h, která stanovuje pravidla pro vysílání v pásmu 5GHz.

Mezi připravované normy patří například standard 802.11k a 802.11n. Standard „k“ má sloužit k měření a správě radiových zdrojů tak, aby vyhovovaly novým bezdrátovým sítím. Standard „n“ má přinést zcela průlomové zvýšení rychlosti ve WLAN. Cílem je nabídnout uživatelům reálnou rychlost 100 Mb/s a hovoří se dokonce o rychlostech až 320 Mb/s. Stávajících 54 Mb/s, resp. reálných cca 30 Mb/s standardu 802.11g nevyhovuje vysokým nárokům uživatelů. [3]

Podrobnější vysvětlení jednotlivých standardů a principu fungování WIFI bude uvedeno v následující kapitole.

3.2 Dělení a princip činnosti WIFI

Technologie WIFI pracuje na dvou frekvenčních pásmech – jedno je kolem kmitočtu 2.4 GHz a druhé kolem 5.5 GHz. Na kmitočtech kolem 2.4 GHz pracují například standardy „b“ a „g“ a na kmitočtech kolem 5.5 GHz pracuje například standard „a“.

Přesný rozsah kmitočtu kolem 2.4 GHz je 2,412 až 2,484 GHz . V pásmu kolem 5,5 GHz to vypadá následovně – 5,150 až 5,250 , dále pak 5,150 až 5,350 a dále 5,470 až 5,725 a také 5,725 až 5,825 GHz. Toto dělení je podle toho, v jaké oblasti se WIFI technologie používá – viz následující dělení :

- Japonsko : 5,150 až 5,250 GHz
- USA : 5,150 až 5,350 GHz – pro venkovní použití, 5,725 až 5,825 GHz pro vnitřní
- Evropa : 5,150 až 5,350 GHz – pro vnitřní použití, 5,470 až 5,725 GHz pro venkovní

Pro kmitočty kolem 2,4 GHz existuje také podobné dělení – dělí se na různé pracovní kanály – těchto kanálů je celkem 14. Každý kanál má 5 MHz kromě posledního čtrnáctého, který je určen pro Japonsko a má 12 MHz. Vypadá to tedy následovně – 1. kanál – 2,412 GHz, 2. kanál – 2,417 GHz atd., 13. kanál – 2,472 a 14. kanál – 2,484 GHz.

- USA a Kanada – 1. až 11. kanál – 2,412 až 2,462 GHz
- Evropa mimo Francie a Španělska – 1. až 13. kanál – 2,412 až 2,472 GHz
- Francie – 10. až 13. kanál – 2,457 až 2,472 GHz
- Španělsko – 10. až 11. kanál – 2,457 až 2,462 GHz
- Japonsko – 14. kanál – 2,484 GHz

3.2.1 Jednotlivé vrstvy ISO/OSI

- **Aplikační –** Stará se o přenos informací mezi programy.
- **Prezentační –** Zobrazování a konverze přenesených dat.
- **Relační –** Koordinace a udržování spojení.
- **Transportní –** Řízení doručování informací a kvality přenosu.
- **Síťová –** Obsluha přenosových tras a zpráv.
- **Spojová(Linková) –** Zabývá se kódováním a přenosem informací.
- **Fyzická –** Zajišťuje komunikaci na nejnižší úrovni – v podstatě řeší vlastní propojení hardwaru(karet).

Obrázek č. 13 – model iso/osi

Nejdůležitější vrstvou pro přenos dat mezi prvky sítě je tedy fyzická vrstva – PHY. Je to fyzické rozhraní mezi zařízeními v síti. Jedná se tedy o bezdrátovou vrstvu, která popisuje jakým způsobem se šíří rádiový signál v síti WIFI.

3.2.2 Fyzická vrstva

Když byl v roce 1997 stanoven původní standard 802.11, obsahoval tři standardy fyzické vrstvy. V roce 1999 byly přidány další dva standardy fyzické vrstvy.

1997 :

- Frequency - hopping (FH) spread - spectrum radio PHY
- Direct – sequence (DS) spread – spectrum PHY
- Infračervené světlo (IR) PHY

1999 :

- Orthogonal Frequency Division Multiplexing (OFDM) PHY
- High – Rate Direct Sequence (HR / DS nebo HR/ DSSS) PHY

Rozprostřené spektrum

Technologie rozprostřeného spektra (SS – spread spectrum) se používá pro dosažení rychlých datových přenosů v pásmu ISM. Tradiční rádiové technologie se soustředí na vměšování co největšího počtu signálů do relativně úzkého pásma. Oproti tomu rozprostřené spektrum používá matematické funkce pro rozptýlení síly signálu do širokého frekvenčního bloku. Přijímač pak jednoduše provede opačnou operaci a složí signál zpět do klasického úzkého pásma, se kterým dále pracuje.

Na principu rozprostřeného spektra jsou právě založené i některé standardy fyzické vrstvy – a to Frequency – hopping, Direct – sequence a Orthogonal Frequency Division Multiplexing.

3.2.2.1 Frequency hopping (Frekvenční poskoky)

Tato technika má vojenský původ. Vysílač skáče v pseudonáhodném pořadí po jednotlivých frekvenčních pásmech a na každém tomto pásmu vysílá krátký datový proud. V České Republice je dostupná frekvenční šířka 83,5 MHz – tato šířka je rozdělena do 75 nebo 79 frekvenčních kanálů o šířce 1 MHz. Zbylých 4,5 MHz slouží jako ochranné pásmo. Rádiový signál pak skáče v pseudonáhodném pořadí po těchto kanálech tak, že každých 30 sekund musí vystřídat alespoň 75 kanálů a na každém smí vysílat maximálně 400 milisekund. Výhodou frekvenčních proskoků je větší počet systémů pracujících najednou v pásmu 2,4 Ghz. Nevýhodou však je omezení rychlosti na 2Mb/s.

3.2.2.2 Direct sequence (Přímá sekvence)

Využívá se přímé sekvence rozprostřené po 22 MHz širokém frekvenčním pásu vysílanou informaci za použití matematického kódování. Celková šířka pásma je 83,5 MHz a tedy k dispozici máme tři 22. MHz pásma. Přijímač inverzním postupem signál dekóduje. Původní standard 802.11 definuje fyzickou vrstvu DS o rychlosti 2Mb/s, standard 802.11b pak přímou sekvenci (HR/DSSS) o rychlosti až 11Mb/s.

3.2.2.3 OFDM (Ortogonální frekvenční multiplex)

Systém rozdělí přenosové pásmo na velké množství úzkých kanálů, data se v každém kanálu přenášejí relativně pomalu a signál je tak mnohem robustnější. Ve výsledku je ale rychlost přenosu dat součtem všech kanálů, tedy až 54 Mb/s. Vrstva OFDM byla přijata jako standard 802.11a, tedy pro pásmo ISM 5GHz a později adaptována pro pásmo ISM 2,4 GHz jako standard 802.11g.

3.2.2.4 Podvrstvy fyzické vrstvy PLCP, PMD, MAC

- **Protokol konvergence fyzické vrstvy** (PLCP –Physical Layer Convergence Procedure)
- **Závislá od fyzického média** (PMD –Physical Medium Dependent)
- **MAC** (Media Access Control)

PMD se stará o kódování bezdrátového přenosu, tedy o přenos každého bitu z podvrstvy PLCP do éteru pomocí antény.

PLCP představuje spojení mezi přenášenými rámci MAC podvrstvy (popsána v kapitole 3.) a přenosovým médiem. Procedura PLCP připojuje k přenášeným rámcům vlastní hlavičku v závislosti na použité metodě modulace, díky této vrstvě je tedy přenášený rámec nezávislí na metodě použité modulace. Mimo jiné poskytuje funkci CCA (Clear Channel Assessment), jenž dává odezvu pro podvrstvu MAC, že přenosové medium je k dispozici.

Formát PLCP

PLCP se skládá z preambule a hlavičky. Standard definuje dva druhy preambule a to krátkou a dlouhou. Všechny systémy splňující standard musí podporovat dlouhou preambuli, krátká je určena pro zvýšení propustnosti sítě při přenosu větších dat například při videokonferencích či přenosu zvuku.
Preambule obsahuje synchronizační pole 128bitů u dlouhé a 56 bitů u krátké. Dále 16 bitový oddělovač začátku rámce SFD (Start Frame Delimiter), který se používá pro označení počátku každého rámce.

Hlavička PLCP obsahuje:

- 8 bitové pole DR (Data Rate field) pro určení datové rychlosti
- 8 bitů vyhrazených pro budoucí použití
- 16 bitové políčko udávající velikost přenášených dat, tedy nese informace o délce MAC PDU (Medium Access Control Protocol Data Unit)
- 16 bitů tvoří poslední pole hlavičky PLCP nazvané HEC (Header Error Check) jeho úloha je vyloučit chybu v PLCP hlavičce pomocí kontrolního součtu bytů v CRC kódu.

MAC (Media Access Control)

Tato podvrstva slouží jako rozhraní mezi fyzickou vrstvou a hostitelským zařízením, vytváří také podporu ad-hoc a infrastrukturního zapojení sítě.

Formát MAC rámce

Rámec se skládá ze tří částí hlavičky, těla a kontrolního součtu. Hlavička je dále rozdělena na 7 částí viz. tabulka č.5.

2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration / ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

Hlavička

Tabulka č. 5 : Formát MAC rámce (čísla nad tabulkou značí počty bajtů jednotlivých polí)

Popis jednotlivých polí MAC rámce:

- **Frame Control** – obsahuje informace o verzi protokolu a typu rámce.
- **Duration/ID** – ID je identifikátor stanice používaný pro funkci úspory energie.
  - Duration Value je délka trvání rámce pro výpočet rezervace přenosového média pomocí Network Allocation Vector (NAV).
- **Address 1- 4** – čtyři adresní pole obsahující adresy zdroje,cíle přenašeče a přijímače v závislosti na poli Frame Control.
- **Sequence Control** – toto 16 bitové pole obsahuje dvě podpole.
  - Fragment Number - 4bitové pole indikující číslo fragmentace
  - Sequence Number – 12 bitové pole číslo indikující sekvenci čísel, slouží pro identifikaci a likvidaci duplicitních rámců
- **Frame Body** – pole obsahující přenášená data.

FCS - obsahuje 32 bitové CRC (Cyclic Redundancy Check) neboli cyklický kontrolní součet, který slouží ke zjištění zda paket nebyl během přenosu poškozen. Kontrolní součet je vypočítáván ze všech polí MAC hlavičky a Frame Body podle polynomu. CRC doplní každý přenášený rámec o zbytek po dělení polynomem (FCS), přičemž zabezpečován je celý rámec včetně znaku začátku rámce. Pro zabezpečení se používají následující polynom:

$$G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

Struktura Frame Control

Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order
2	2	4	1	1	1	1	1	1	1	1

Tabulka č. 6: Struktura Frame Control - čísla pod políčky jsou konkrétní počty bitů

Protokol Version – pole o velikosti dvou bitů udává verzi protokolu, pro základní standard 802.11 odpovídá 0, ostatní hodnoty jsou rezervovány, pro případné nekompatibilní specifikace standardu.

Type a Subtype – kombinace těchto dvou poli, udává typ a podtyp rámce. Typy rámců jsou control, data, management (kontrolní, datový, řídící). Bližší popis možných hodnot těchto dvou polí viz. standard 802.11.

To DS - je nastaveno na 1, pokud je rámec posílán do distribučního systému, tedy všechna data směřující ze stanice do přístupového bodu. Ve všech ostatních případech je pole To DS nastaveno na 0.

From DS – je nastaveno na 1, pokud je rámec přijímán od distribučního systému.

To DS = 0 From DS=0	Datový rámec přenášený mezi dvěma stanicemi
To DS = 1 From DS = 0	Datový rámec určený pro distribuční systém
To DS = 0 From DS= 1	Datový rámec přicházející z distribučního systému
To DS = 1 From DS= 1	Datový rámec přenášený mezi dvě přístupovými body

Tabulka č. 7: Možné kombinace To/From DS polí

More Fragment – je nastaveno na 1, pokud byl přenášený rámec rozdělen na více částí přenášených samostatně.

Retry – je-li nastaveno na 1 jedná se o znovu-vysílání již vysílané části rámce, přijímač tak pozná duplicitní rámce.

Power Management – nastavení na 1 znamená že se stanice po přenesení dat bude nacházet v režimu úspory energie.

More Data – 1 oznamuje, že je ve vyrovnávací paměti pro tuto stanici uloženo více dat.

WEP – nastavení na 1 znamená, že tělo rámce je kódováno algoritmem WEP

Order – 1 indikuje že rámec je odesílán službou Strict-Ordering, tedy nebude dále zpracováván.

3.2.3 Jednotlivé Standardy

IEEE 802.11a – popisuje práci WIFI zařízení v pásmu 5 GHz. Začalo se na ní pracovat dříve než na normě „b“, ale díky větší složitosti přenosu signálu v pásmu 5 GHz byla ukončena později než norma „b“. Dovoluje teoretickou rychlost až 54 Mbit za sekundu – prakticky je ale možné dosáhnou 30 až 36 Mbit za sekundu a to v takzvaném turbo režimu. Pro dosažení takovéto rychlost bylo poprvé použito Orthogonal Frequency-Division Multiplexing – OFDM.

IEEE 802.11b - Přenos probíhá v pásmu 2,4 až 2,4835 GHz (rozsah 83,5 MHz). Šířka pásma je v České Republice rozdělena na 13 kanálů. Aby se signál jednotlivých kanálů nerušil, je nutné nastavit je tak, aby pracovaly minimálně 5 kanálů od sebe (např. 1, 6, 11). Teoretická přenosová rychlost je 11 Mbit za sekundu. Tento standard spolu s 802.11g se u nás neuvěřitelně rychle rozšířil a ve větších městech je již problém s umístěním vlastního AP, aby jste nerušily některé z okolních sítí.

IEEE 802.11c – Tato vrstva se zabývá činností komunikačních mostů na úrovni podvrstvy MAC (Media Access Control) 802.11 a je doplňkem k mezinárodní normě IS 10038 (IEEE 802.1D) o transparentních mostech (konkrétně protokolu Spanning Tree Protocol, STP). Doplněk byl schválen v roce 1998.

IEEE 802.11d – Tato norma byla přijata v roce 2001. Upravuje normu 802.11b a to pro použití v místech, kde není pásmo 2,4 GHz dostupné – upravuje normu „b“ pro použití v jiných kmitočtových pásmech.

IEEE 802.11e – Tato norma zatím nebyla schválena. Norma „e“ doplňuje podporu pro kvalitu služeb QoS (s využitím Time Division Multiple Access - TDMA) a opravu chyb do podvrstvy MAC na podporu všech fyzických vrstev používaných v IEEE 802.11 sítích, kromě ad-hoc(bude vysvětleno později) typů sítí.

IEEE 802.11f - Vylepšuje mechanismus předávání stanic (roaming) při přechodu mezi dvěma rádiovými kanály nebo z jedné sítě do sousední s připojením k jinému přístupovému bodu. Má také umožnit spolupráci přístupových bodů od různých výrobců – k tomu má sloužit protokol IAPP (Inter-Access Point Protocol).

IEEE 802.11g – Tato norma se stala nástupcem normy „b“. Je s ní také zpětně kompatibilní. Byla schválena v roce 2003. Na rozdíl od normy „b“ je schopná poskytnout teoretickou přenosovou rychlost až 54 Mbit za sekundu. Je také kompatibilní se všemi doplňkovými normami jako 802.11d - internacionalizace, 802.11e - kvalita služeb a 802.11i - bezpečnost. Fyzická vrstva je řešena pomocí OFDM (Orthogonal Frequency-Division Multiplexing), podobně jako 802.11a. Pro zpětnou slučitelnost s 802.11b podporuje také CCK (Complementary Code Keying); volitelně rovněž modulaci PBCC (Packet Binary Convolution Coding) jako ústupek vůči Texas Instruments (nepřináší nic nového).

IEEE 802.11h – Tato norma vylepšuje řízení využití kmitočtového spektra (výběr kanálu a řízení vysílacího výkonu) a doplňuje tak normu 802.11a. Evropští regulátoři požadují pro schválení produktů 802.11a použití dynamického výběru kanálu (Dynamic Channel Selection, pro venkovní i vnitřní komunikaci) a řízení vysílacího výkonu (Transmit Power Control) u zařízení pracujících na kmitočtu 5 GHz. Norma 802.11h má právě tyto možnosti doplnit do normy 802.11a. Tyto doplňky se budou týkat pouze pásma 5 GHz, nikoli 2,4 GHz.

IEEE 802.11i – Tato norma doplňuje bezpečnostní prvky na úrovni fyzické podvrstvy MAC. Místo šifrovacího protokolu WEP (Wireless Encryption Privacy) je použit nový způsob šifrování: Advanced Encryption Standard (AES).

IEEE 802.11j – Tato norma představuje nové řešení koexistence 802.11a a HIPERLAN/2 na stejných vlnách. HIPERLAN/2 je evropská norma (ETSI) využívající pásmo 5 GHz a podporující rychlosti (na fyzické vrstvě) do 54 Mb/s. Mezi výhody HIPERLAN/2 patří, že používá OFDM a má zabudovanou podporu pro QoS (řešení fyzické vrstvy totiž vychází z bezdrátového Asynchronous Transfer Mode, ATM). Specifikace pro HIPERLAN/2 ještě nebyla schválena, očekává se až v příštím roce, podobně jako produkty na ní založené. [6] [16]

A další normy :

Norma	Rok schválení	Popis
802.11k	2006	Měření rádiových prostředků.
802.11n	2008*	Vysoká propustnost.
802.11p	2007*	Bezdrátový přístup pro mobilní zařízení.
802.11r	2007*	Rychlý roaming.
802.11u	2007*	Spolupráce s externími sítěmi.
802.11.2	2008*	Měření a testování WLAN zařízení.
802.11v	2008*	Management bezdrátových zařízení.
802.11s	2008*	Multi-hopping.
802.11w	2008*	Podpora integrity, autenticity a ochrany dat.

*** – standard nebyl doposud schválen, údaj určuje předpokládaný rok schválení**

Příklady základních parametrů dnes nejrozšířenějších standardů jsou vidět v následující tabulce č. 8:

Standard	Pásmo [GHz]	Maximální rychlost [Mbit/s]	Fyzická vrstva
IEEE 802.11 původní	2,4	2	DSSS
IEEE 802.11a	5	54	OFDM
IEEE 802.11b	2,4	11	DSSS
IEEE 802.11g	2,4	54	OFDM
IEEE 802.11n zatim neni standardizován	2,4 nebo 5	540	OFDM, MIMO

Tabulka č. 8 : Nejpoužívanější standardy

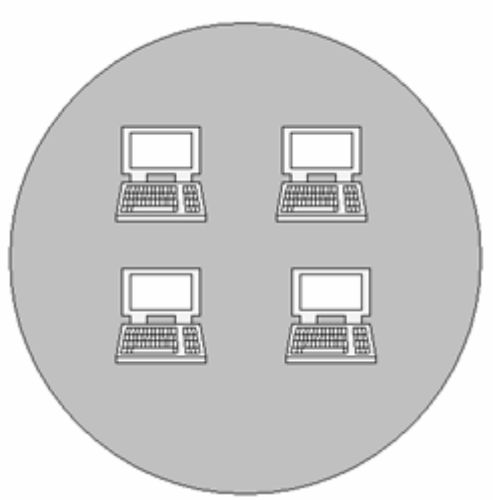
3.3 Topologie sítí WIFI

Nejrozšířenější WIFI sítě lze vybudovat dvěma základními způsoby :

- Sítě Infrastrukturní - založené na přístupovém bodu – Access pointu
- Sítě ad-hoc – vznikne tak síť pear to pear

3.3.1 AD – HOC

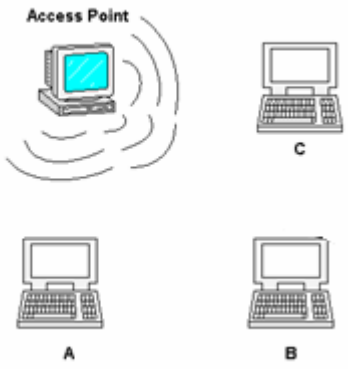
V sítích tohoto typu mezi sebou komunikují zařízení bez nutnosti použití prostředníka(přístupového bodu). Pokud spolu stanice chtějí komunikovat musí být ve vzájemném rádiovém dosahu. V praxi se tento typ sítě používá pro propojení jen několika málo počítačů a to jen na omezený čas – obrázek 14, například při nárazové výměně dat. Každý klient je vlastně samostatným přístupovým bodem. Takto nezávislá síť se pak nazývá Independent Service basic set – IBSS.



Obrázek č. 14 : Síť AD-HOC

3.3.2 Infrastrukturní sítě - řízené přístupovým bodem

Tyto sítě se také někdy označují jako sítě s infrastrukturou. Obsahují minimálně jeden přístupový bod – takzvaný access point – obrázek 15. Tato základní stanice je připojena většinou pomocí kabelu do klasické sítě LAN. Může ale pracovat i bez připojení do sítě LAN. Jednotliví klienti nekomunikují vzájemně mezi sebou, ale využívají k tomu právě tohoto přístupového bodu. Přístupové body a klienti se dělí o šířku pásma. Často dnes můžeme v těchto sítích vidět takzvaný Wireless LAN BroadBand Router – zařízení, které nabízí možnost připojení k internetu. Obsahuje také většinou několik portů LAN, přes něž je pomocí kabelů možné připojit několik dalších klientů.Tyto sítě se také někdy nazývají Basic Service Set – BSS. [20] [22] [23]



Obrázek č. 15 : Síť s přístupovým bodem

3.4 Koordinace přístupu k médiu

Za médiu je zde považováno prostředí ve kterém se šíří signál. Koordinace přístupu k médiu potom zajišťuje která stanice bude v daném okamžiku komunikovat s přístupovým bodem nebo s jinou stanicí – tedy řeší situace kdy k médiu chce přistupovat více stanic – pokud by přistupovalo více stanic naráz, docházelo by ke kolizím a přístupový bod by pravděpodobně komunikoval se stanicí s nejsilnějším signálem. Toto by samozřejmě znemožňovalo funkci sítě. Proto se tato situace řeší.

Standard 802.11 řeší tento problém pomocí dvou funkcí pro koordinaci přístupu k médiu :

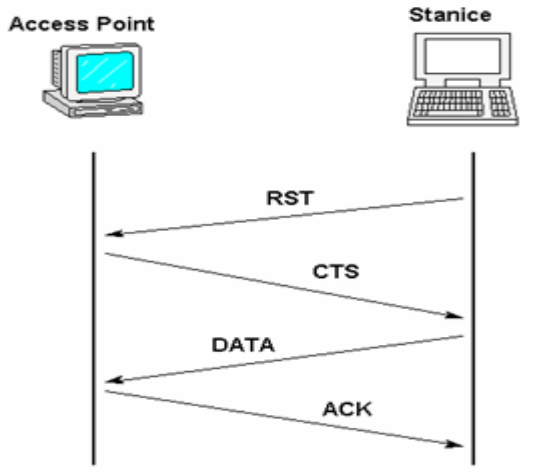
- DFC – funkce distribuované koordinace
- PCF – funkce koordinace jedním bodem

Právě funkce DFC tvoří základ přístupového mechanismu CSMA/CA. Funkce PCF se používá v aplikacích blížících se reálnému času. V případě použití PCF přiděluje přístupový bod každé stanici prioritu přístupu k médiu pro určený přenosový rámec. Funkce PCF není ale ještě rozšířena. Více se používá funkce DFC.

Jak již bylo řečeno DFC tvoří základ pro mechanismus CSMA/CA, která je podobná mechanismu CSMA/CD u ethernetu. U CSMA/CD řeší tento mechanismus detekci kolizí, zatímco mechanismus CSMA/CA se těmto kolizím snaží předcházet a to prostřednictvím čtyř rámců – příklad komunikace je znázorněn na obrázku č. 16.

- RST (Request to send)
- CTS (Clear to send)
- ACK (Acknowledge)
- NAV (Network allocation vector)

Komunikaci ilustruje obrázek . Stanice naslouchá a pokud je medium volné, počká ještě určený čas (DIFS) a teprve potom začne vysílat. Aby se předešlo kolizím stanice nejprve vyšle řídící paket RST obsahující kromě zdroje a cíle i trvání následujícího přenosu. Cílová stanice odpoví řídícím paketem CTS obsahujícím dobu trvání následujícího přenosu. Ostatní stanice které slyší pakety RTS nebo CTS si nastaví indikátor virtuálního naslouchání (NAV) na dobu trvání přenosu oznámenou v paketu. Po tuto dobu bude brát stanice médium jako obsazené. Vysílající stanice potom vyšle data. Přijímající stanice zkontroluje kontrolní součet CRC přijatého paketu a odešle potvrzení ACK. Pokud stanice paket ACK neobdrží opakuje vysílaní.



Obrázek č. 16 : Příklad komunikace

Pro koordinaci přístupu k médiu definuje standard 802.11 čtyři typy mezer mezi rámci (Inter Frame spacing- IFS) :

- **Short Interface Space (SIFS)** – nejkratší mezirámcová mezera, používá se pro bezprostřední odpovědi – ACK, odpověď na výzvu.

- **Point Coordination Function (PIFS)** - používá se pro výzvy. Má přednost před normálním provozem.

- **Distributed IFS (DIFS)** - nejdelší IFS, minimální prostoj při soupeření asynchronních rámců o přístup. Stanice má přístup k médiu v okamžiku, kdy toto bylo volné po dobu delší než trvání DIFS.

- **Extended IFS (EIFS)** – používá se pouze tehdy, pokud je chyba v přenosu rámce.

3.5 Bezpečnost WIFI sítí

Data se v bezdrátových sítích vysílají všesměrově a tak není težké je odposlechnout. Pro zabezpečení bezdrátových sítí instituce IEEE 802.11 navrhla šifrování v podobě protokolu WEP (Wired Equivalent Privacy), což v překladu znamená "bezpečnost odpovídající drátu". Snaha byla o to aby nebyl při šifrování zatížen hardware. Kvůli tomu byla použita slabší šifra.

3.5.1 Protokol WEP

Tento protokol zajišťuje šifrování rámců na síťové vrstvě. Provádí šifrování veškerých rámců mezi klientem a přístupovým bodem. K šifrovaní se používá algoritmus RC4, jehož autorem je R. Rivest a zveřejněn byl v roce 1994. Používá proudovou symetrickou šifru s délkou klíče 40, 104, 232 bitů. V roce 2001 však bylo v algoritmu objeveno hned několik bezpečnostních nedostatků. Slabinou tohoto algoritmu je to, že pro šifrování a dešifrování musí mít klient někde uložený klíč – výrobci některých karet ho implementují přímo do hardwaru, ale není to tak vždy – existují i případy kdy byl klíč uložen v registrech. K šifrování se však délka klíče buď nafoukne nebo zmenší – podle délky zprávy. Zpráva je potom zašifrována pomocí operace XOR a dešifrována reverzně. Proto je tedy možné po odposlechnutí komunikace rozluštit pomocí operace XOR klíč, kterým je komunikace zašifrována. Zašifrování stejné zprávy symetrickou šifrou totiž pokaždé generuje stejnou šifrovanou zprávu a tím pádem je mnohem jednoduší klíč uhodnout. Proto je součástí WEP ještě inicializační vektor (IV), který se mění s každým paketem a doplňuje klíč o dalších 24 bitů. Při použití WEPu s klíčem dlouhým 128 bitů má klíč pouze 104 bitů + 24 bitů IV. Generování IV zajišťuje vysílací strana, která ho nejenom použije k sestavení šifrovaného streamu, ale přidá ho v otevřené podobě i do záhlaví rámce.

I když má protokol WEP mnoho nedostatků je dnes nejpoužívanějším zabezpečovacím protokolem WIFI sítí. Kombinuje se s dalšími bezpečnostními prvky – jako třeba filtrování MAC adres, přiřazování IP adres ručně – vypnutím DHCP serveru nebo zakázáním SSID broadcastingu – identifikace sítě – bude vysvětleno později.

3.5.2 Protokol WPA

Je založen stejně jako WEP na šifrovacím algoritmu RC4. Cílem protokolu WPA bylo odstranit nedostatky protokolu WEP. Na rozdíl od WEP používá 128 bitový dynamický klíč, který se mění každých 10000 paketů. Dalším zlepšením je MIC (Message Integrity Check), jež je používán současně s CRC32 a tím řeší jeho nedostatky, díky kterým bylo možné změnit zprávu při zachování stejného kontrolního součtu. [10] [11]

Protokol WPA-TKIP (Temporal Key Integrity Protocol)

U standardu 802.11 je šifrování WEP (Wired Equivalent Privacy) nepovinné. Standard WPA vyžaduje šifrování pomocí protokolu TKIP. Protokol TKIP nahrazuje šifrování WEP novým šifrovacím algoritmem, který je silnější než algoritmus WEP, k provádění šifrovacích operací však používá výpočetní možnosti existujících bezdrátových zařízení. Protokol TKIP obsahuje také následující funkce:

- ověření platnosti konfigurace zabezpečení po určení šifrovacích klíčů
- synchronizovaná změna šifrovacího klíče jednosměrového vysílání pro jednotlivé rámce
- určení jedinečného počátečního šifrovacího klíče jednosměrového vysílání u každého ověřování předsdílených klíčů

3.6 SSID

Každý přístupový bod vysílá každých 100 milisekund administrativní signalizaci(beacon), kterou o sobě dává vědět všem WIFI zařízením, které jsou v dosahu. Tato vysílaná zpráva obsahuje různé informace o přístupovém bodu – například SSID – Service Set Identifier neboli název sítě, dále číslo kanálu na kterém pracuje, způsob zabezpečení – WEP nebo WPA nebo nic, dále podporované rychlosti, sílu signálu a další parametry.
[4] [21]

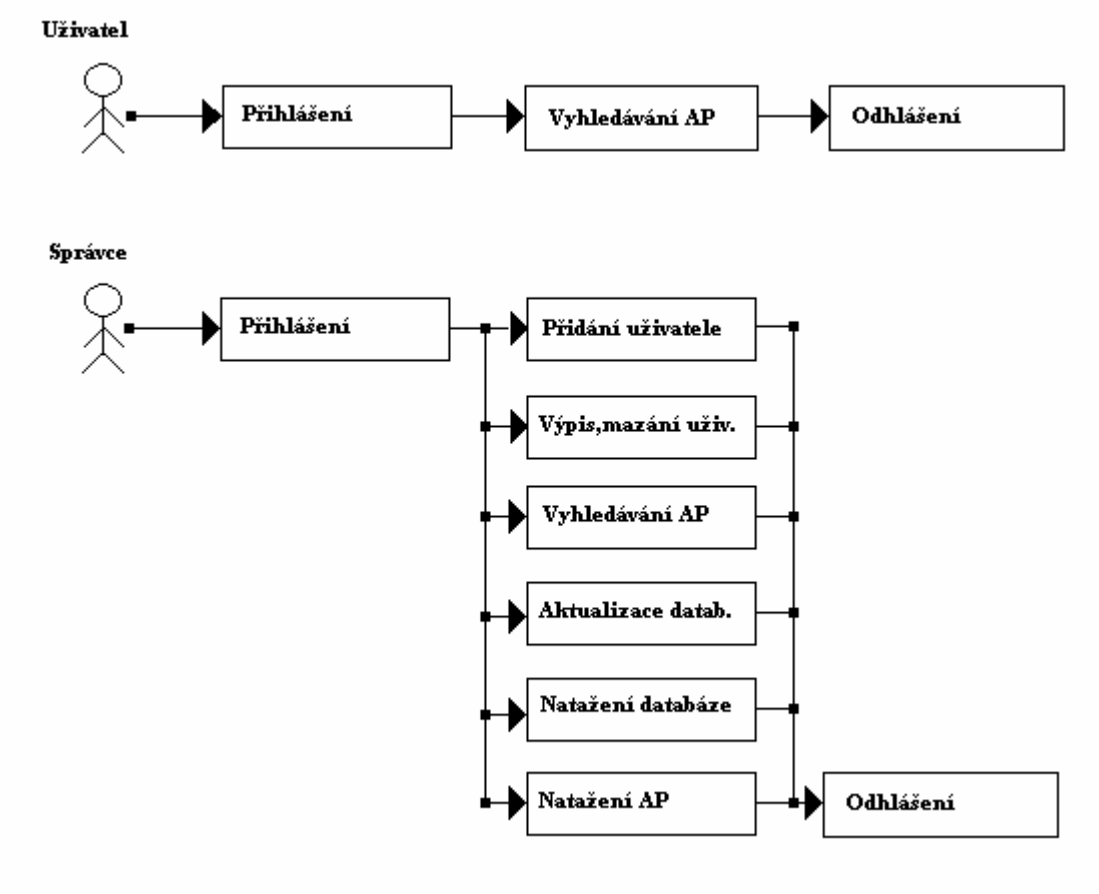
4. Závěr teoretické části

Na parametrech SSID a na geografické poloze poskytnuté GPS přijímačem je založena má diplomová práce. Jednotlivé parametry budou uloženy do speciálního typu souboru – soubor bude používat pouze znaky ASCII – nejprve budou uloženy data o SSID – jednotlivé parametry budou odděleny speciálním znakem „#“ a závorkami. Poslední parametry budou tvořit informace o poloze – souřadnice X, souřadnice Y, a výška. Z těchto parametrů budou potom odhadnuty polohy přístupových bodů a kompletní informace o jednotlivých přístupových bodech budou uloženy do jednoduché databáze.

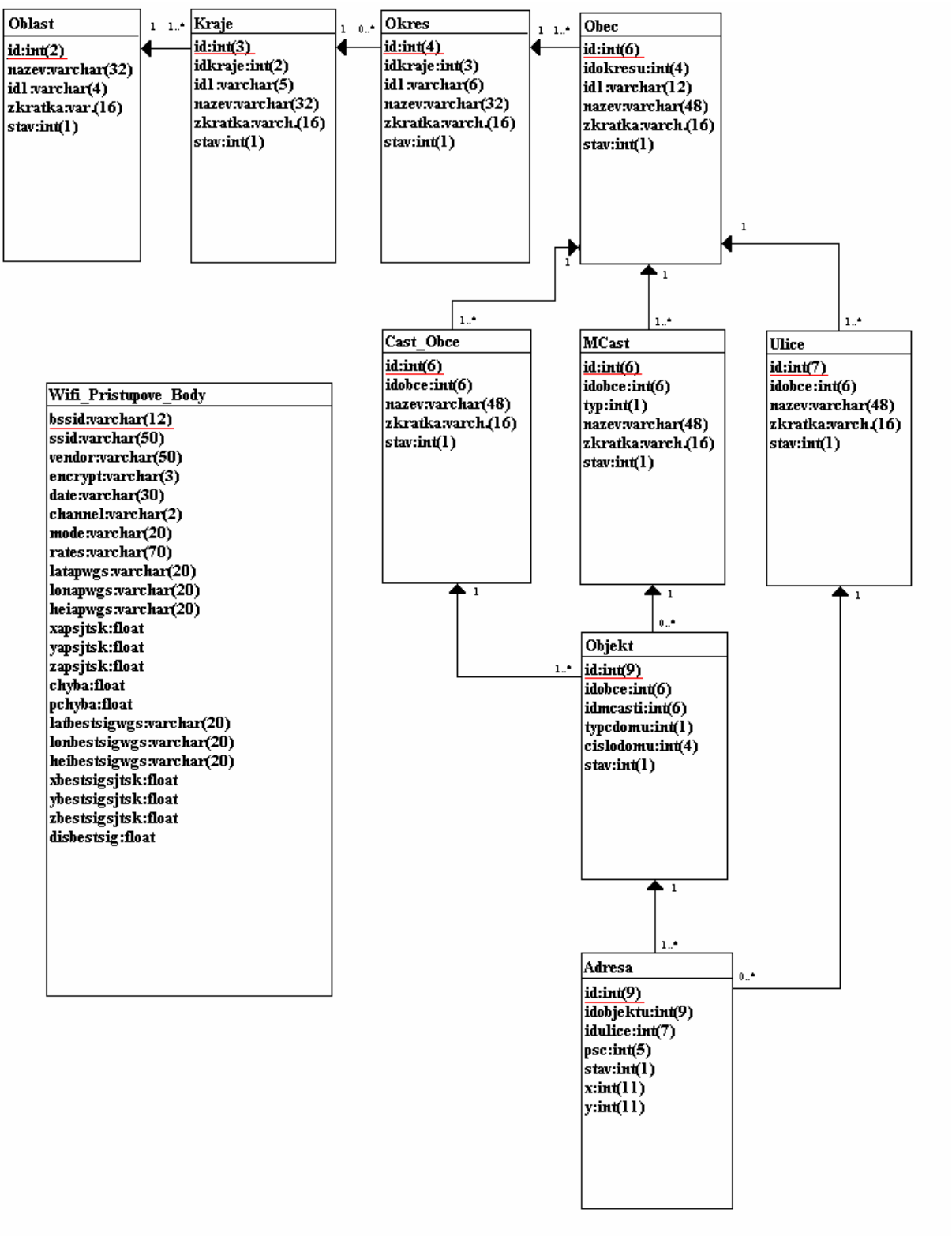
5. Návrh řešení a databáze

Informace o jednotlivých přístupových bodech budu získávat pomocí volně dostupných nástrojů – viz implementace. Tyto data budu zpracovávat a polohu přístupových bodů budu počítat pomocí vytvořeného nástroje v programovacím nástroji "Delphi". Vytvořená data budu zpracovávat přes webové rozhraní, přes které budou tyto data o přístupových bodech uložena do navržené databáze. Přes toto webové rozhraní bude také možné jednotlivé přístupové body vyhledávat.

Úkolem mojí diplomové práce také bylo, aby bylo možné jednotlivé přístupové body hledat podle zadané lokality – části území – například ulice, části obce a podobně. Inspirovat jsem se měl už vzniklými databázemi přístupových bodů. Po dlouhém hledání na internetu a zjištění přibližné podoby, obsahu a struktury těchto databází jsem dále musel řešit problém, kde získat potřebná data pro to, abych takovéto vyhledávání přístupových bodů mohl realizovat. Při pročítání různých diskusních stránek jsem narazil na projekt Ministerstva práce a sociálních věcí nazvaný „UIR-ADR" [27] - Územně identifikační registr adres. Je to vlastně databáze všech oblastí, krajů, okresů, měst, obcí, ulic, objektů a adres a mnoha dalších pro mě už méně významných věcí. Důležité je, že je tato databáze na požádání volně dostupná, volně šířitelná, jsou k dispozici volně stažitelné aktualizace a tabulka „Adresy" v této databázi obsahuje gps souřadnice jednotlivých adres v souřadném systému SJTSK. Při návrhu vlastní databáze jsem tedy vycházel z databáze „UIR-ADR", ke které jsem ještě navíc přidal tabulku reprezentující jednotlivé přístupové body. Na obrázku č. 18 je znázorněn ER – diagram navržené databáze a na obrázku č. 17 je znázorněn diagram použití.



Obrázek č. 17 – diagram případů užití



Obrázek č. 18 – ER diagram databáze

6. Implementace

6.1 Úvod

Ke své diplomové práci využívám několik volně dostupných nástrojů. Celkový proces "výpočtu" probíhá tak, že jsou zároveň spuštěné programy *netstumbler* , *cain* a můj program nazvaný *mojegps*. Všechny tyto tři programy běží souběžně a to tak, že nejdříve musí být spuštěn program *mojegps*- vysvětleno bude později. Volně dostupné programy *netstumbler* a *cain* se starají o zaznamenávání informací o dostupných přístupových bodech a program *mojegps* se stará o zaznamenávání souřadnic gps. Programy *netstumbler* a *mojegps* se zároveň starají o zaznamenávání přesného časového údaje – jsou časově synchronizované a na základě této časové synchronizace jsou jednotlivé exporty ze všech použitých nástrojů propojeny. Takže výstupem těchto tří nástrojů jsou tři vyexportované soubory které obsahují informace o přístupových bodech, záznam gps pozic a časový údaj jak u gps pozic tak u záznamů informací o jednotlivých přístupových bodech.

Dále je použit další můj vytvořený nástroj, který provede sloučení a protřídění těchto tří vyexportovaných souborů a souhrnné informace společně s vypočítanou pozicí jednotlivých přístupových bodů uloží do jednoho výstupního souboru.

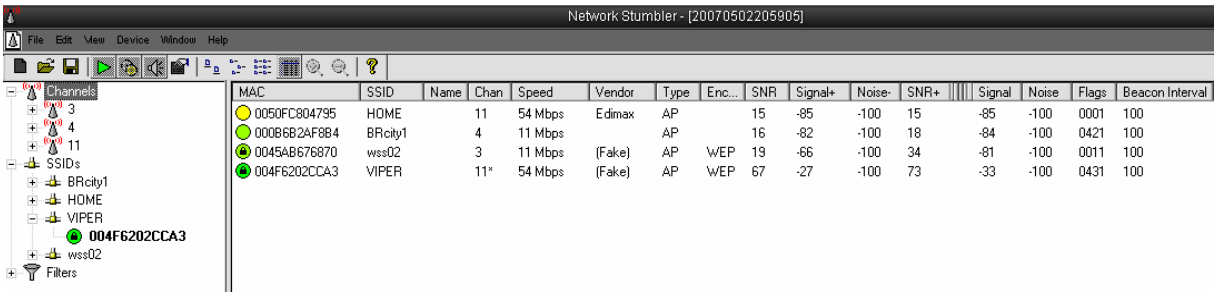
Tento výstupní soubor je dále zpracován php skriptem, který jednotlivé záznamy uloží do databáze, která kromě tabulky s informacemi o přístupových bodech obsahuje data a informace o ulicích, obcích, městech, krajích …. Tuto databázi jsem získal na žádost od Ministerstva práce a sociálních věcí [27] – tato databáze je volně šířitelná. Navíc obsahuje SJTSK souřadnice jednotlivých adres takže je možné určovat například jaké přístupové body se nacházejí na jednotlivých ulicích atd..

Jednotlivé formáty exportovaných souborů, struktura a popis výstupního souboru a podrobný popis databáze včetně popsání jednotlivých použitých nástrojů a postup a způsob provedení mého řešení a mých výpočtů podrobně popíši v následujících kapitolách.

6.2 Použité nástroje

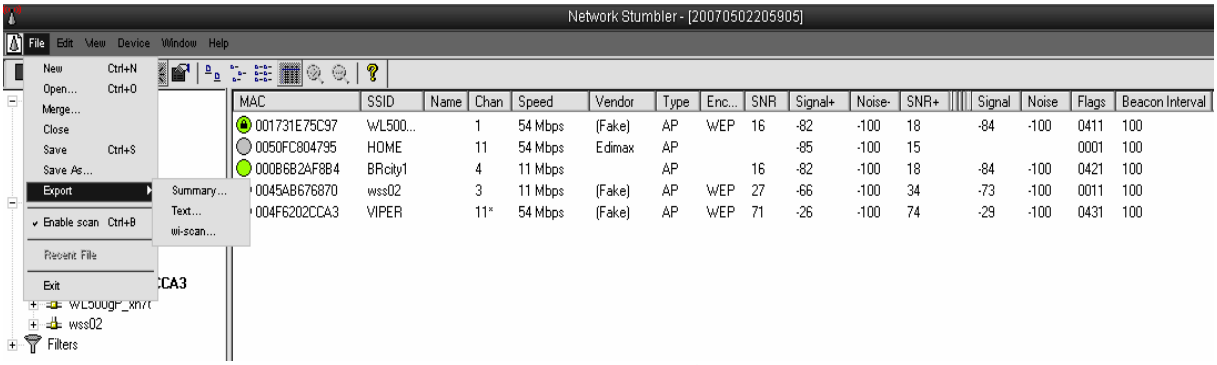
6.2.1 Netstumbler

Tento volně dostupný nástroj [24] je schopen spolupracovat s wi-fi síťovou kartou a je schopen pomocí ní monitorovat jednotlivé přístupové body, které jsou v dosahu této síťové karty. Při monitorování zobrazuje nejdůležitější data, které jednotlivé přístupové body vysílají a které sám odvodí nebo získá ze síťové karty – mezi nejdůležitější informace patří MAC adresa(BSSID), název(SSID), popis přístupového bodu(VENDOR), čas(TIME), odstup signálu od šumu(SNR), útlum signálu(SIGNAL), šum(NOISE), pracovní kanál(CHAN). Tyto informace a ještě pár dalších je vidět okamžitě po započetí monitorování – viz obrázek č.19.



Obrázek č. 19 – obrazovka *netstumbleru*

Program je ale také schopen provádět export jednotlivých informací do externích souborů – obrázek č. 20.



Obrázek č. 20 – export souborů z *netstumbleru*

Konkrétně umí exportovat tři druhy souborů – „summary", „text" a „wi-scan" . Do souboru „summary" exportuje celkový pohled na provedené monitorováni – takže každému přístupovému bodu je v tomto souboru přidělen jeden záznam(řádek), který obsahuje některé z výše uvedených informací – unikátní je BSSID neboli MAC adresa. Na obrázku č.21 můžete vidět výpis části z vyexportovaného souboru „summary".

```
( SSID )       Type    ( BSSID )       Time (GMT)      [ SNR Sig Noise ]      # ( Name )     Flags   Channelbits     BcnIntvl        DataRate

( Kvik-3Com )  BSS     ( 00:0f:cb:fc:35:12 )   12:42:14 (GMT)  [ 36 85 49 ]    # (  )  0431    00000800        100     540     11
( default )    BSS     ( 00:50:fc:d7:21:ae )   12:42:14 (GMT)  [ 41 90 49 ]    # (  )  0001    00000800        100     110     11
( default )    BSS     ( 00:15:f2:90:17:71 )   12:42:14 (GMT)  [ 54 103 49 ]   # (  )  0401    00000002        100     540     1
(  )    BSS    ( 00:15:f2:08:e0:e0 )   12:42:14 (GMT)  [ 40 89 49 ]    # (  )  0431    00000002        100     540     1
( JiH.net )    BSS     ( 00:14:bf:e3:22:55 )   12:42:14 (GMT)  [ 26 75 49 ]    # (  )  0411    00000040        100     540     6
( NCITYbone2 ) BSS     ( 00:02:2d:20:93:02 )   12:42:14 (GMT)  [ 35 84 49 ]    # (  )  0011    00000100        100     110     8
( Colombo )    BSS     ( 00:12:0e:26:9b:8d )   12:42:14 (GMT)  [ 30 79 49 ]    # (  )  0011    00000200        100     110     9
( Bzenda )     BSS     ( 00:e0:98:52:b1:58 )   12:42:14 (GMT)  [ 32 81 49 ]    # (  )  0431    00000800        100     540     11
( Frantiska )  BSS     ( 00:0e:2e:a1:7d:02 )   12:42:14 (GMT)  [ 37 86 49 ]    # (  )  0411    00000800        100     540     11
( MadPixel )   BSS     ( 00:11:50:1a:1a:5f )   12:42:14 (GMT)  [ 33 82 49 ]    # (  )  0401    00000008        100     540     3
```

Obrázek č. 21 – soubor *summary* z *netstumbleru*

Z obrázku č. 18 je tedy vidět část struktury vyexportovaného souboru „summary" , který obsahuje různé informace – viz výše. Nejdůležitější pro mou diplomovou práci jsou informace BSSID, SSID, TIME, SNR, SIG, NOISE. Jelikož je ale tento soubor pouze shrnutím provedeného monitorování a data v něm jsou obsažená i v dalším vyexportovaném souboru, tak tento soubor k získání informací nepoužívám.

Dalším exportovaným souborem je soubor s označením „text". Tento soubor už je pro mou diplomovou práci zajímavější, protože obsahuje celý záznam informací k jednotlivým

přístupovým bodům v každém časovém úseku(po sekundách) – je to vlastně takový podrobný zápis celého provedeného monitorování – takže pokud byl v určitém čase v dosahu nějaký přístupový bod pak má v tomto souboru záznam s informacemi a s daným časovým „razítkem". Tento soubor jako jediný z těch tří, které dokáže „netstumbler" exportovat používám ve své diplomové práci ke zjištění a získání základních informací a dat o přístupových bodech v lokalitě, ve které jsem monitorování přístupových bodů prováděl. Struktura a informace obsažené v tomto souboru jsou podrobně znázorněné na obrázku č. 22 na kterém je znázorněn pouze výsek ze souboru „text".

```
( SSID )        Type    ( BSSID )       Time (GMT)      [ SNR Sig Noise ]       # ( Name )      Flags   Channelbits     BcnIntvl        DataRate

( Kvik-3Com )   BSS     ( 00:0f:cb:fc:35:12 )   12:42:14 (GMT)  [ 20 69 49 ]    # (  )  0431    00000800        100     540     11
( Gauneri )     BSS     ( 00:17:9a:f0:fb:87 )   12:42:14 (GMT)  [ 40 89 49 ]    # (  )  0431    00000040        100     540     6
( default )     BSS     ( 00:15:f2:90:17:71 )   12:42:14 (GMT)  [ 46 95 49 ]    # (  )  0401    00000002        100     540     1
( www802cz5644openDHCP )        BSS     ( 00:11:95:e6:55:4b )   12:42:14 (GMT)  [ 20 69 49 ]    # (  )  0401    00000002        100     110     1
( Frantiska )   BSS     ( 00:0e:2e:a1:7d:02 )   12:42:14 (GMT)  [ 19 68 49 ]    # (  )  0411    00000800        100     540     11
( Mambo )       BSS     ( 00:12:0e:2d:9c:56 )   12:42:14 (GMT)  [ 34 83 49 ]    # (  )  0011    00000200        100     110     9
(  )    ????    ( 00:90:cc:26:1e:88 )   12:42:14 (GMT)  [ 23 72 49 ]    # (  )  0030    00000100        100     10      8
( Vinohrady )   BSS     ( 00:15:f2:3b:36:b3 )   12:42:14 (GMT)  [ 24 73 49 ]    # (  )  0401    00000002        100     540     1
( Bzenda )      BSS     ( 00:e0:98:52:b1:58 )   12:42:14 (GMT)  [ 19 68 49 ]    # (  )  0431    00000800        100     540     11
( Guanako Wi-Fi )       BSS     ( 00:0e:2e:92:22:29 )   12:42:14 (GMT)  [ 26 75 49 ]    # (  )  0411    00000800        100     540     11
( Colombo )     BSS     ( 00:12:0e:26:9b:8d )   12:42:14 (GMT)  [ 17 66 49 ]    # (  )  0011    00000200        100     110     9
( w1qw-b4 )     BSS     ( 00:13:46:74:14:be )   12:42:14 (GMT)  [ 19 68 49 ]    # (  )  0431    00000008        100     110     3
```

Obrázek č. 22 – soubor *text* z *netstumbleru*

Jak je vidět z obrázku č. 22, tak každý záznam je umístěn na samostatném řádku – celý soubor tedy zpracovávám po řádcích a potom z jednotlivých řádků získávám informace v daném čase – na obrázku zrovna čas 12:42:14 a k nim stav jednotlivých přístupových bodů.

Jako posledním exportovaným souborem je soubor s označením „wi-scan", který obsahuje stejně jako předchozí soubor celý záznam monitorování – obsahuje i některé stejné informace, ale některé neobsahuje – je to takový „chudší bráška" předchozího souboru. Struktura a obsah tohoto souboru je vidět na obrázku č. 23.

```
# $Creator: Network Stumbler Version 0.4.0
# $Format: wi-scan
# Latitude      Longitude       ( SSID )        Type    ( BSSID )       Time (GMT)      [ SNR Sig Noise ]
# $DateGMT: 2007-04-10
N 0.0000000     E 0.0000000     ( Kvik-3Com )   BBS     ( 00:0f:cb:fc:35:12 )   12:42:14 (GMT)  [ 20 69 49 ]
N 0.0000000     E 0.0000000     ( NCITYbone2 )  BBS     ( 00:02:2d:20:93:02 )   12:42:14 (GMT)  [ 17 66 49 ]
N 0.0000000     E 0.0000000     ( NCITYbone50 ) BBS     ( 00:0f:a3:42:18:67 )   12:42:14 (GMT)  [ 19 68 49 ]
N 0.0000000     E 0.0000000     ( Colombo )     BBS     ( 00:12:0e:26:9b:8d )   12:42:14 (GMT)  [ 17 66 49 ]
N 0.0000000     E 0.0000000     ( Bzenda )      BBS     ( 00:e0:98:52:b1:58 )   12:42:14 (GMT)  [ 19 68 49 ]
N 0.0000000     E 0.0000000     (  )    BBS     ( 00:15:f2:08:e0:e0 )   12:42:14 (GMT)  [ 23 72 49 ]
N 0.0000000     E 0.0000000     ( NCITYbone50 ) BBS     ( 00:0f:a3:42:19:2b )   12:42:14 (GMT)  [ 28 77 49 ]
N 0.0000000     E 0.0000000     (  )    BBS     ( 00:13:f7:0f:3a:00 )   12:42:14 (GMT)  [ 20 69 49 ]
N 0.0000000     E 0.0000000     ( Frantiska )   BBS     ( 00:0e:2e:a1:7d:02 )   12:42:14 (GMT)  [ 19 68 49 ]
N 0.0000000     E 0.0000000     ( Guanako Wi-Fi )       BBS     ( 00:0e:2e:92:22:29 )   12:42:14 (GMT)  [ 26 75 49 ]
N 0.0000000     E 0.0000000     ( Mambo )       BBS     ( 00:12:0e:2d:9c:56 )   12:42:14 (GMT)  [ 34 83 49 ]
```

Obrázek č. 23 – soubor *wi-scan* z *netstumbleru*

Jak je vidět na obrázku č. 23, tak soubor „wi-scan" obsahuje i informace o poloze monitorování – Latitude a Longitude. Tyto informace obsahuje i předešlý soubor, ale já je ve své diplomové práci nepoužívám, protože zde není zaznamenána výška, která je potřebná pro přepočítání souřadnic ze souřadného systému WGS-84 na pravoúhlý souřadný systém používaný v České Republice a to SJTSK. Převod z jednoho souřadného systému do druhého provádím proto, že v systému WGS-84 nelze se souřadnicemi pravoúhle počítat – tzn. , že nelze například spočítat pomocí Pythagorovy věty vzdálenost dvou bodů. Proto pro záznam jednotlivých souřadnic v daném čase používám svůj vlastní program, jehož

výsledkem po skončení monitorování je výstupní soubor, který obsahuje získané polohy vztažené k jednotlivým časovým razítkům. [24]

Popis tohoto programu včetně jeho funkce, struktury a obsahu výstupního souboru bude uveden v následujících kapitolách.

6.2.2 Cain

Další volně dostupný nástroj [25], který jsem použil se stará o doplnění některých informací o přístupových bodech, které nástroj „netstumbler“ nedává k dispozici ve vyexportovaných souborech. Jsou to informace o rychlostech(RATES), které přístupový bod podporuje a informace o tom jestli je komunikace s přístupovým bodem šifrována(ENCRYPT) či nikoli. Výstupem tohoto nástroje je jeden vyexportovaný soubor označený jako „cain“, jehož obsah a strukturu je možné vidět v tomto krátkém výpisu.

Výpis ze souboru *Cain* :

```
================================================================
= Cain's Wireless Scanner                                      =
================================================================
BSSID: 000FCBFC3512
Last seen: 10/04/2007 - 14:47:47
Vendor: 3COM EUROPE LTD
Signal: -64 dBm
SSID: Kvik-3Com
Enc: Yes
Mode: Infrastructure
Channel: 11 (2462000 Hz)
Rates (Mbps): 1, 2, 5, 6, 9, 11, 12, 18,
Packets:
Unique WEP IVs:

BSSID: 0050FCD721AE
Last seen: 10/04/2007 - 15:20:09
Vendor: EDIMAX TECHNOLOGY CO., LTD.
Signal: -74 dBm
SSID: default
Enc: No
Mode: Infrastructure
Channel: 11 (2462000 Hz)
Rates (Mbps): 1, 2, 5, 11,
Packets:
Unique WEP IVs:
```

Soubor „cain“ má podobný obsah jako soubor „summary“ z nástroje „netstumbler“. Také obsahuje pouze sumu celého monitorování – takže každý dostupný přístupový bod zde má jeden záznam v podobě 11. řádků – jak je vidět z předchozího výpisu. Propojení ostatní vyexportovaných souborů s tímto souborem provádím přes jednoznačný identifikátor každého přístupového bodu a tím je BSSID, neboli MAC adresa. Z každého záznamu o přístupovém bodu v tomto souboru získávám informace LAST SEEN, RATES, ENC. [25]

6.2.3 *MojeGPS*

Poslední nástroj který používám k celkovému měření(monitorování) je mnou vytvořený program v prostředí DELPHI. Úkolem tohoto programu je po celou dobu monitorování sekundu po sekundě zjišťovat gps polohu jak v souřadném systému WGS-84 tak i přepočítávat tyto souřadnice do souřadného systému SJTSK. Oba dva typy souřadnic potom s přesným systémovým časem, který používá i nástroj „netstumbler“ ukládá do výstupního souboru jehož strukturu a obsah můžete vidět na obrázku č. 24. Ke komunikaci s gps modulem používám volně dostupnou komponentu pro delphi nazvanou „GPS“ [26].

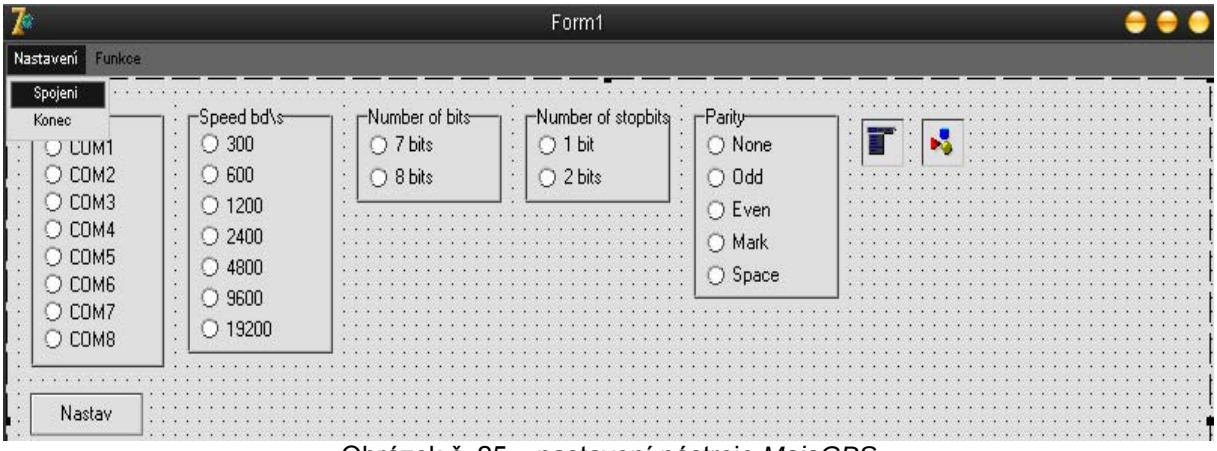
Tato komponenta je schopná každou sekundu vracet informace o vaší poloze, počtu viditelných satelitů, kvalitě signálu a o velikosti signálu.

```
cas$14:41:56#sirka$49.207846667#delka$16.659088333#kvalita$Normal#vyska$331.400#geovyska$43.500#pocetsatelitu$5#x$1159743.80580477#y$594308.684514599#z$286.9
cas$14:41:57#sirka$49.207831667#delka$16.659058333#kvalita$Normal#vyska$329.400#geovyska$43.500#pocetsatelitu$5#x$1159745.23080526#y$594311.035955177#z$284.9
cas$14:41:58#sirka$49.207830000#delka$16.659055000#kvalita$Normal#vyska$329.000#geovyska$43.500#pocetsatelitu$5#x$1159745.38917649#y$594311.297203816#z$284.5
cas$14:41:59#sirka$49.207831667#delka$16.659056667#kvalita$Normal#vyska$328.900#geovyska$43.500#pocetsatelitu$5#x$1159745.21783473#y$594311.156638359#z$284.4
cas$14:42:00#sirka$49.207848333#delka$16.659085000#kvalita$Normal#vyska$330.600#geovyska$43.500#pocetsatelitu$6#x$1159743.59565346#y$594308.906166368#z$286.1
cas$14:42:01#sirka$49.207861667#delka$16.659106667#kvalita$Normal#vyska$331.800#geovyska$43.500#pocetsatelitu$6#x$1159742.2899956#y$594307.178172746#z$287.39
cas$14:42:02#sirka$49.207871667#delka$16.659125000#kvalita$Normal#vyska$332.800#geovyska$43.500#pocetsatelitu$6#x$1159741.32701753#y$594305.731304853#z$288.3
cas$14:42:03#sirka$49.207878333#delka$16.659133333#kvalita$Normal#vyska$333.200#geovyska$43.500#pocetsatelitu$6#x$1159740.65483625#y$594305.04846132#z$288.79
cas$14:42:03#sirka$49.207878333#delka$16.659133333#kvalita$Normal#vyska$333.200#geovyska$43.500#pocetsatelitu$6#x$1159740.65483625#y$594305.04846132#z$288.79
cas$14:42:04#sirka$49.207878333#delka$16.659133333#kvalita$Normal#vyska$333.000#geovyska$43.500#pocetsatelitu$6#x$1159740.65483451#y$594305.048458594#z$288.5
cas$14:42:05#sirka$49.207870000#delka$16.659116667#kvalita$Normal#vyska$331.900#geovyska$43.500#pocetsatelitu$6#x$1159741.44647087#y$594306.354760974#z$287.4
cas$14:42:06#sirka$49.207863333#delka$16.659105000#kvalita$Normal#vyska$331.100#geovyska$43.500#pocetsatelitu$6#x$1159742.09281131#y$594307.279135927#z$286.6
```

Obrázek č. 24 – výstupní soubor nástroje *MojeGPS*

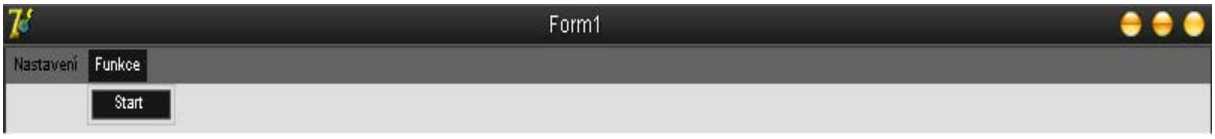
Na obrázku č. 24 je tedy jako první informace znázorněn systémový čas, informace sirka, delka a vyska se týkají souřadného systému WGS-84. Parametry x,y,z se týkají souřadného systému SJTSK. Parametr geovyska určuje výšku nad referenčním geoidem – viz teoretická část. Poslední dva parametry jsou kvalita signálu a počet viditelných satelitů – podle tohoto údaje se později provádí „pročištění“ naměřených dat – pokud je počet satelitů menší jak 4 – viz. teorie, pak není takový záznam brán v potaz při dalších výpočtech.

Ovládání a nastavení tohoto programu je jednoduché. Nejdříve je potřeba nastavit parametry spojení s gps modulem – v mém případě je to usb modul značky NAVILOCK, model NL-302U. Veškeré nastavení se ukládá do souboru, takže není nutné při každém spuštění znovu tyto parametry nastavovat. Jaké parametry se nastavují je znázorněno na obrázku č. 25.



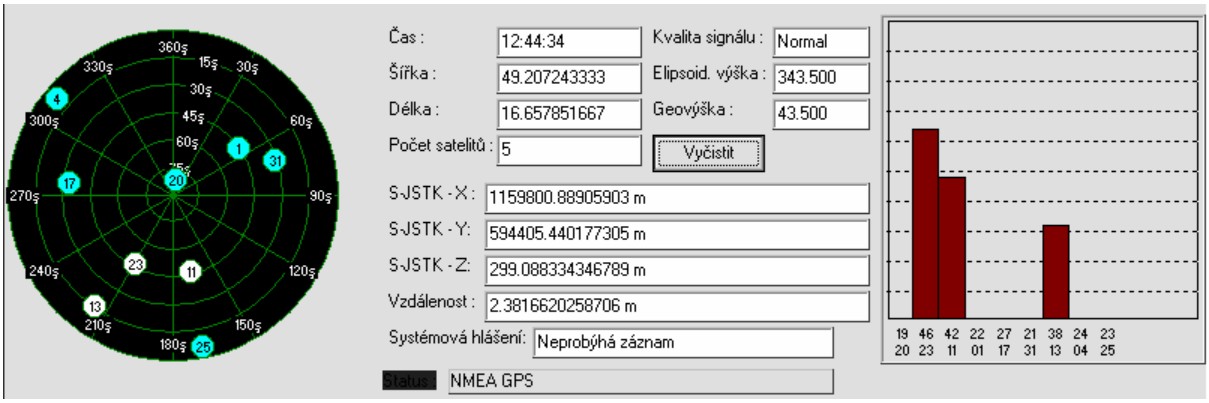
Obrázek č. 25 – nastavení nástroje *MojeGPS*

Jak je vidět z obrázku č. 25 tak se nastavuje číslo portu, přenosová rychlost, počet bitů – „přenesených naráz“, počet stop bitů a paritu. Vlastně nastavujete parametry komunikace po sériové lince, protože gps modul komunikuje s PC pomocí RS-232. V mém případě jsou hodnoty nastavení rovny – *Port = COM4*, *SPEED = 4800 bd/s*, *NUMBER OF BITS = 8*, *NUMBER OF STOPBITS = 1* a *PARITY = NONE*. Po nastavení těchto parametrů už můžete zahájit práci – obrázek č.26.



Obrázek č.26 – spuštění funkce nástroje MojeGPS

Po stisku tlačítka start začne program zobrazovat informace – viz výše. Tyto informace jsou znázorněné na obrázku č. 27.



Obrázek č. 27 – nástroj MojeGPS

Nyní program pouze zobrazuje získané informace, ale nikam je neukládá. Pro to aby začal program zaznamenávat data do výstupního souboru je potřeba stisknout tlačítko „zaznam“ – viz obrázek č. 28.

Obrázek č. 28 – záznam výstupního souboru nástroje *MojeGPS*

Po stisku tohoto tlačítka se začne záznam do souboru „soubor_gps.log“, který je umístěn ve stejném adresáři jako samotný program. Převzaté algoritmy pro převod mezi souřadnými systémy uvedu později.

6.2.4 GPS_WI-FI

Předešlé tři nástroje sloužily k získání informací o přístupových bodech a o čase a přesné gps poloze v jednotlivých časových úsecích. Výstupem těchto tří nástrojů jsou tři vyexportované soubory. Další mnou vytvořený nástroj s označením *GPS_WI-FI* tyto tři soubory zpracuje a spojí do jednoho výstupního souboru, který bude dále zpracován php skriptem, který jeho data uloží do databáze – o databázi později.

Zpracování těchto tří vstupních souborů od předchozích nástrojů probíhá v několika fázích. **V první fázi** se zpracuje soubor označený jako „cain“ – viz výše – vyberou se z něj důležité informace a uloží se do pomocného souboru, jehož obsah a struktura je vidět na následujícím výpisu.

Výpis z pomocného souboru :

```
#BSSID(000FCBFC3512)#SSID(Kvik-3Com)#VENDOR(3COM EUROPE
LTD)#ENCRYPT(Yes)#DATE(10/04/2007)#CHANNEL(11)#MODE(Infrastructure)#
RATES(1, 2, 5, 6, 9, 11, 12, 18, )#
```

Takto vypadá jeden řádek, tedy záznam o jednom přístupovém bodu – jednotlivé zkratky nebudu znovu popisovat – jsou uvedeny výše. Nejdůležitější informací v tomto záznamu je BSSID neboli MAC adresa přístupového bodu, která je pro každý přístupoví bod jedinečná.

Ve druhé fázi zpracování vstupních souborů se zpracovává vstupní soubor s označením „text“ od nástroje *netstumbler* a vstupní soubor s označením „soubor_gps.log“ od nástroje *mojegps*. Z obsahu obou těchto souborů je vidět, že oba obsahují záznamy s časovými razítky. Na základě těchto časových razítek jsou oba soubory propojeny a výsledek(jejich spojení) je uložen do dalšího pomocného souboru. Spojení těchto dvou souborů probíhá tak, že se soubor s označením „text“ čte řádek po řádku – tedy po jednotlivých záznamech a z každého takového záznamu se získá časové razítko. Takto získané časové razítko se potom hledá v souboru označeném jako „soubor_gps.log“ a tím dojde k přiřazení gps informací k jednotlivým záznamům s informacemi o přístupových bodech – včetně systémového času kdy takový záznam při monitorování vznikl. Příklad této fáze je vidět na obrázku následujícím příkladu.

Příklad :

Část souboru s označením „text“ : Jeden řádek

N 0.0000000 E 0.0000000 (Kvik-3Com) BSS (00:0f:cb:fc:35:12) 14:42:14 (GMT)
[20 69 49] # ( ) 0431 00000800 100 540 11

Nalezený záznam se stejným časem v souboru s označením „soubor_gps.log“ :

cas$14:42:14#sirka$49.207720000#delka$16.658888333#kvalita$Normal#vyska$314.000#geovyska$43.500#pocetsatelitu$7#x$1159756.25423788#y$594324.677526325#z$269.589928555067#

Spojením vznikne záznam, který je uložen do druhého pomocného souboru :

#MAC$000FCBFC3512#TIME$14:42:14#SIGNAL$69#CHANNEL$11#DISTANCE$24#sirka$49,207720000#delka$16,658888333#kvalita$Normal#vyska$314,000#geovyska$43,500#pocetsatelitu$7#x$1159756,25423788#y$594324,677526325#z$269,589928555067#

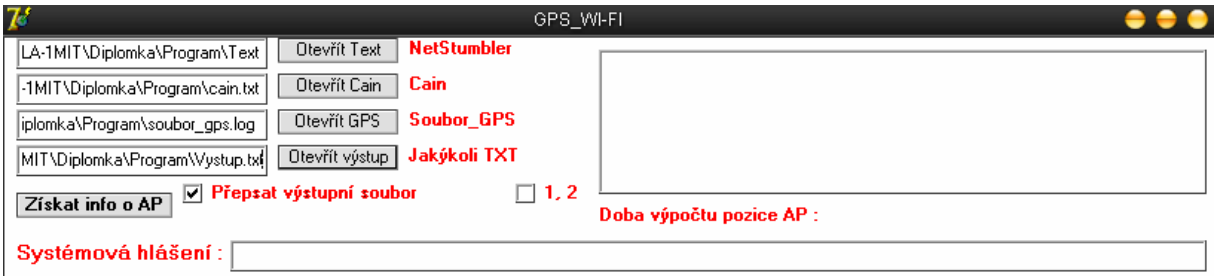
Takovýto záznam tvoří jeden řádek druhého pomocného souboru – identifikátor informace vždy začíná mřížkou a její hodnota vždy začíná dolarem. Ve druhé fázi dochází také k výpočtu vzdálenosti přístupového bodu k místu kde monitorování v daném čase probíhalo. Výpočet vzdálenosti je proveden podle vzorce utlum[dB]=33.5+20*log(f)+20*log(d), kde f je frekvence jednotlivých kanálů a d je vzdálenost v km. Vše potřebné lze získat ze souboru s označením „text“ , takže pomocí jednoduchých úprav lze vzdálenost vypočítat – do druhého pomocného souboru je tato vzdálenost uložena pod identifikátorem *DISTANCE* a hodnota je v metrech. [30] [31]

Třetí fáze dále zpracovává tento druhý pomocný soubor, a to tak, že z něj odstraní všechny záznamy, které vykazují špatnou kvalitu gps signálu nebo je počet satelitů menší než 4. Kvalita signálu se pozná podle parametru *KVALITA* a počet satelitů podle parametru *POCETSATELITU*. Hodnota parametru *KVALITA* nabývá většinou dvou hodnot – jednak hodnoty *NORMAL* a při špatném signálu nabývá hodnoty *NONE* – v takovém případě je záznam odstraněn z tohoto souboru. Také je kontrolována hodnota signálu – pokud nabývá nesmyslné nízké záporné hodnoty, tak je ze souboru tento záznam odstraněn. V průběhu třetí fáze zpracování vstupních souborů tedy vznikne pouze nový, upravený druhý pomocný soubor, který je dále použit ve čtvrté fázi, ve které probíhá výpočet pozic přístupových bodů.

Ve čtvrté fázi zpracování vstupních souborů je zpracováván soubor, který vznikl ve třetí fázi. Nyní už je tedy k dispozici kompletní záznam z celého provedeného monitorování kdy je v jednom souboru obsažena informace o všech přístupových bodech(*BSSID*) a informace o jejich síle signálu na dané pozici v daný čas. Na základě těchto informací se v této fázi

spočítá přibližná poloha přístupového bodu – každému přístupovému bodu se přiřadí vypočítané souřadnice v obou souřadných systémech(WGS-84 i SJTSK), dále se mu přiřadí souřadnice místa ve kterém byl naměřen během monitorování nejlepší signál a takto vytvořená informace se propojí s prvním pomocným souborem, který vznikl v první fázi a uloží se na konečný výstupní soubor tohoto nástroje. Informace, která vznikne ve třetí fázi je s prvním pomocným souborem vzniklým v první fázi propojen na základě jedinečných identifikátorů přístupových bodů, které obě tyto informace obsahují – tedy jak první pomocný soubor tak druhý pomocný soubor – obsah těchto souborů viz výše. Způsob výpočtu polohy přístupového bodu v tomto nástroji bude uveden v jedné z následujících kapitol.

Program s označením *GPS_WI-FI* pracuje následovně – uživatel vybere umístění čtyř souborů – třech vstupních a jednoho výstupního – jak je znázorněno na obrázku č. 29.



Obrázek č. 29 – uživatelské rozhraní nástroje *GPS_WI-FI*

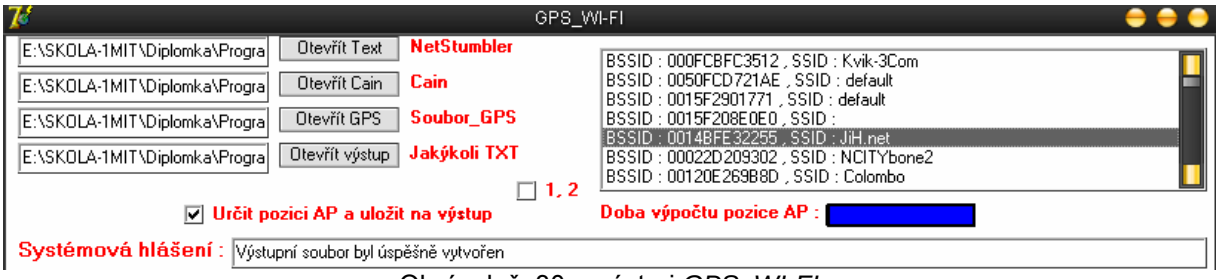
Po stisknutí tlačítka „Získat info o AP“ se na pravé straně okna zobrazí seznam přístupových bodů v podobě MAC adres a názvu přístupového bodu. Dále se zobrazí zaškrtávající políčko „Určit pozici AP a uložit na výstup“. Pokud není zatržené dojde po kliknutí na nějaký přístupový bod v seznamu pouze k vykreslení naměřených dat. Pokud však zaškrtnuté je pak se vykreslí naměřená data také ale zároveň se spočítá pozice přístupového bodu a vše včetně dat z prvního pomocného souboru se uloží do výstupního souboru. Obsah a struktura výstupního souboru je vidět na následujícím výpisu.

Výpis záznamu ze výstupního souboru nástroje *GPS_WI-FI*

```
#BSSID(004F67010A60)#SSID(Misak)#VENDOR()#ENCRYPT(Yes)#DATE(10/04/2007)#CHA
NNEL(11)#MODE(Infrastructure)#RATES(1, 2, 5, 11, 6, 9, 12, 18, )#LATAP(N
49°12m26,968s)#LONAP(E16°39m32,664s)#HEIGHTAP(305)#XAP(1159783)#YAP(594314)
#ZAP(261)#CHYBA(967)#PRUMCHYBA(9)#BESTSIGLAT(N 49°12m28,704s)
#BESTSIGLON(E16°39m31,836s)#BESTSIGHEI(329)#BESTSIGX(284)#BESTSIGY(594324)
#BESTSIGZ(284)#BESTDIS(34)#
```

Na předchozím výpisu je vidět jeden záznam výstupního souboru – obsahuje veškeré informace o přístupovém bodu. Význam jednotlivých parametrů – *BSSID* – mac adresa přístupového bodu, *SSID* – název přístupového bodu, *VENDOR* – většinou uvádí výrobce přístupového bodu, *ENCRYPT* – uvádí jestli je použit nějaký šifrovací mechanismus – WEP,WPA …, *DATE* – datum provedeného monitorování, *CHANNEL* – kanál na kterém přístupový bod pracuje, *MODE* – viz topologie sítí WIFI, *RATES* – podporované rychlosti, *LATAP* + *LONAP* + *HEIAP* – udávají zeměpisnou šířku + délku + výšku vypočítané polohy přístupového bodu v souřadném systému WGS-84, *XAP* + *YAP* + *ZAP* – udávají souřadnice x + y + z polohy přístupového bodu v souřadném systému SJTSK, *CHYBA* – celková chyba vzdáleností všech měření od polohy přístupového bodu, *PRUMCHYBA* – průměrná chyba všech měření použitých k výpočtu přístupového bodu, *BESTSIGLAT* + *BESTSIGLON* + *BESTSIGHEI* – souřadnice polohy s nejlepším naměřeným signálem daného přístupového bodu v systému WGS-84, *BESTSIGX* + *BESTSIGY* + *BESTSIGZ* - souřadnice polohy s nejlepším naměřeným signálem daného přístupového bodu v systému SJTSK, *BESTDIS* – vzdálenost přístupového bodu od polohy, kde byl naměřen nejlepší signál daného přístupového bodu.

Struktura výstupního souboru vypadá tak, že identifikátor parametru vždy začíná znakem mřížka a hodnota daného parametru je umístěna v závorkách. Ovládání tohoto nástroje a výpis přístupových bodů je znázorněn na obrázku č. 30.

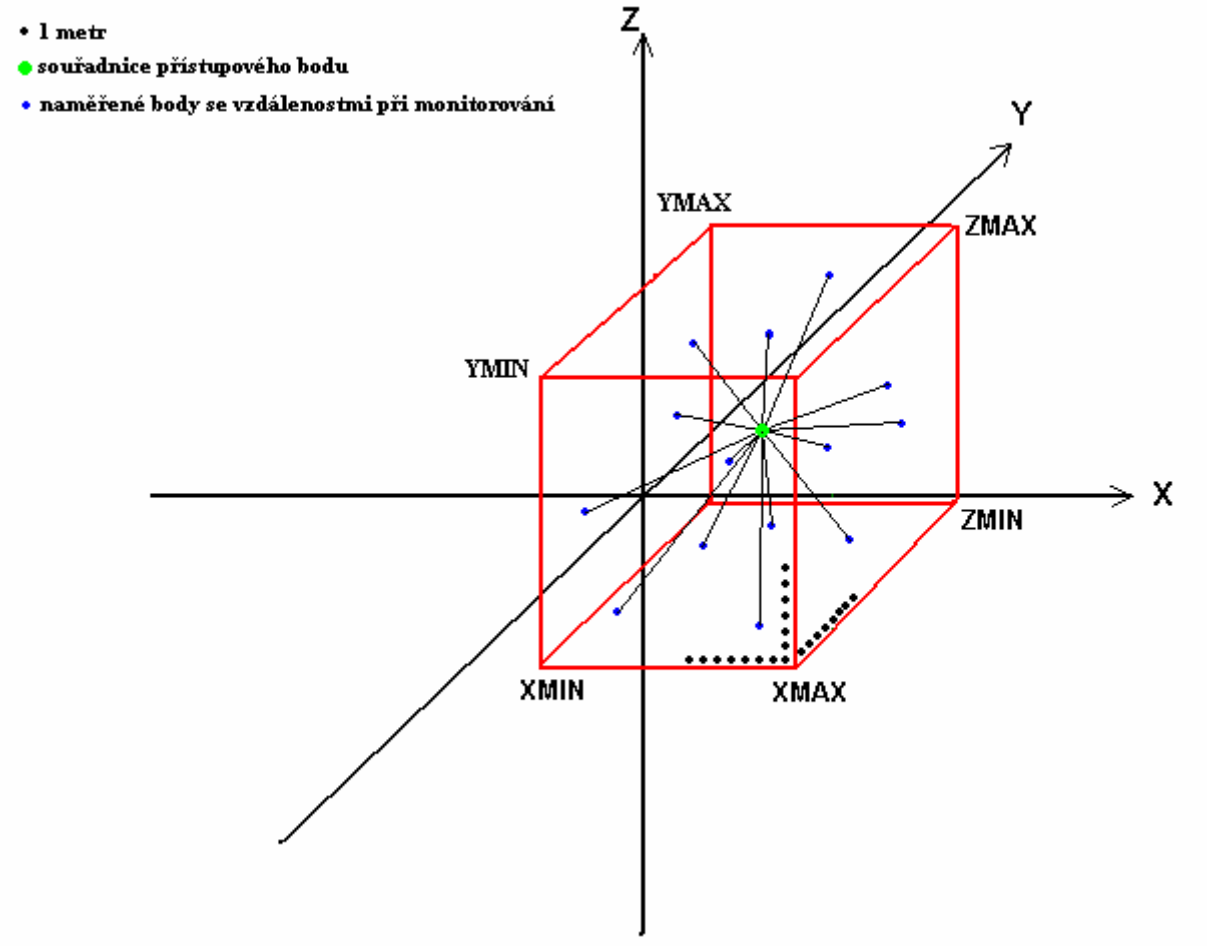


Obrázek č. 30 – nástroj *GPS_WI-FI*

6.3 Výpočet pozice přístupového bodu

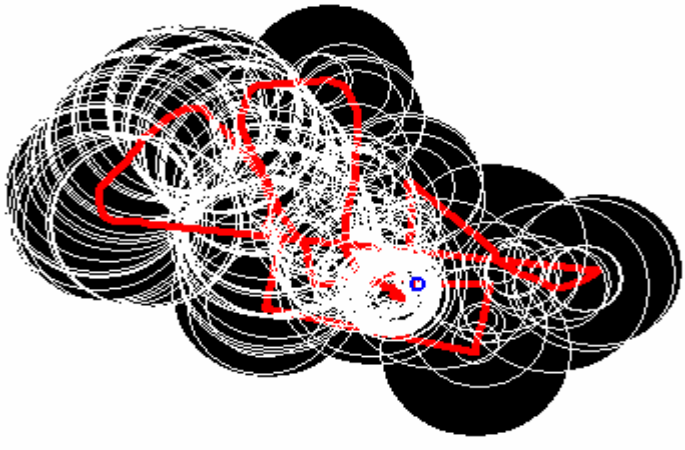
Výpočet pozice přístupového bodu je tedy čtvrtá fáze zpracování vstupních souborů. Počítá se tedy z dat, která vznikla ve třetí fázi – a to hlavně z údajů o poloze jednotlivých měření a vzdálenosti přístupového bodu z této pozice, ve které probíhalo měření. Takže pro každý přístupový bod je ve vstupním souboru několik záznamů(řádků), které obsahují identifikátor přístupového bodu souřadnice a vzdálenost polohy, ze které bylo prováděno monitorování. Souřadnice jsou zde uložené jak v souřadném systému WGS-84 tak v souřadném systému SJTSK. Pro výpočet jsou ale důležité souřadnice v souřadném systému SJTSK, protože se s nimi dá počítat – viz výše.

Vlastní výpočet tedy probíhá tak, že se spočítá jakási mezní hodnota spočítaných vzdáleností a to tak, že se udělá průměr všech naměřených vzdáleností. Tato mezní vzdálenost potom slouží k výběru záznamů, ze kterých se bude počítat poloha přístupového bodu. Pokud je tedy určena mezní vzdálenost začnou se procházet jednotlivé záznamy příslušného přístupového bodu proto, že se určí hranice prostoru, ve kterém bude probíhat výpočet – určí se minimální *x* a maximální *x*, minimální *y* a maximální *y* a minimální *z* a maximální *z*. K těmto minimálním a maximálním hodnotám jsou ještě brány v úvahu jejich vzdálenosti k danému přístupovému bodu – odečtením a přičtením k minimům a maximům. Tímto tedy vznikne prostor ohraničený těmito minimálními a maximálními hodnotami jednotlivých souřadnic souřadného systému SJTSK. Tento prostor se potom prochází metr po metru a počítá se jaký bude součet rozdílů vzdáleností z tohoto bodu k jednotlivým pozicím ve kterých proběhlo monitorování – v naprosto ideálním a dokonalém případě by tento součet byl nulový – tím by byla pozice přístupového bodu určena naprosto přesně. K takové situaci ale nedochází a proto je vybrána pozice z našeho prostoru, ve které bylo dosaženo nejmenšího součtu vzdáleností. Vzdálenost bodu prostoru od naměřených pozic se počítá podle vzorce *((X-X1)^2 + (Y-Y1)^2 + (Z-Z1)^2)^(0.5)*, kde *X,Y,Z* jsou souřadnice bodu v prostoru a *X1,Y1,Z1* jsou souřadnice míst kde probíhalo monitorování. Takto vypočtená vzdálenost se pro každý naměřený bod při monitorování odečte v absolutní hodnotě od vzdálenosti, která byla vypočtena z úrovně signálu v daném změřeném bodě a tato hodnota rozdílu je připočtena k celkové chybě v daném bodě prohledávaného prostoru daného přístupového bodu. Celou situaci znázorňuje obrázek č. 31.



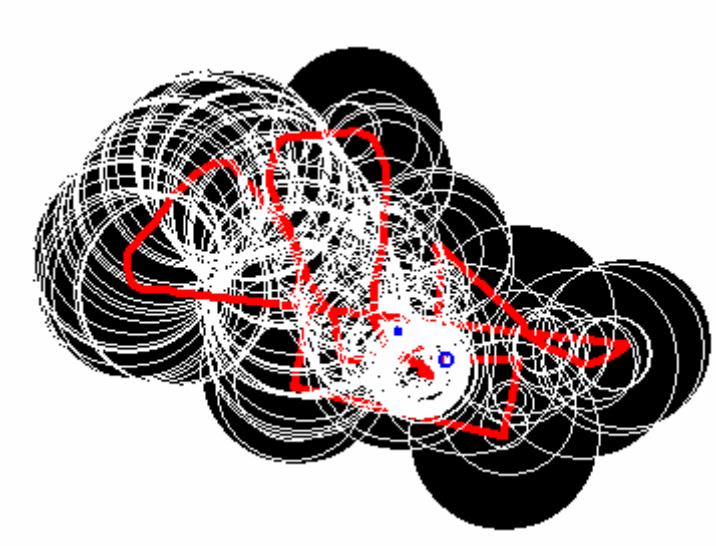
Obrázek č. 31 – výpočet pozice přístupového bodu

Na obrázku č. 31 je vidět ideální případ, kdy se všechny koule se středem v modrých bodech a poloměrem rovným vzdálenosti k přístupovému bodu protnou právě v místě kde je umístěn přístupový bod(zelený bod). Ve skutečnosti tento případ ale nenastává a tyto vypočtené vzdálenosti k přesné pozici přístupového bodu jsou buď větší a nebo menší – proto se v prostoru hledá místo ve kterém je součet rozdílů vzdáleností ze všech naměřených míst v tomto prostoru minimální. To jak vypadá reálně naměřené hodnoty je znázorněno na obrázku č. 32.



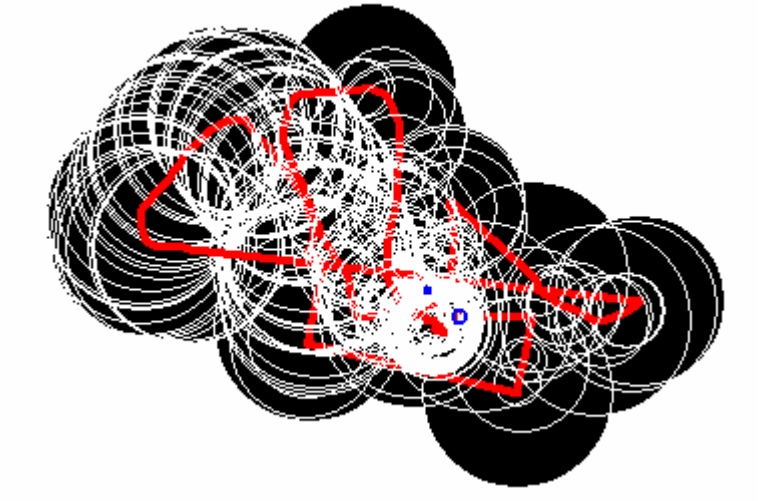
Obrázek č 32 – naměřená data v nástroji *GPS_WI-FI*

Červená čára na obrázku č. 32 je cesta kudy procházel walchalker, který prováděl monitorování. Na této cestě se nacházejí i jednotlivé středy bílých kružnic, které znázorňují vypočítanou vzdálenost k přístupovému bodu – vše je znázorněno v rovině – v reálu by to nebyly kružnice, ale koule – ale pro představu to stačí. Pro představu měřítka se jeden pixel rovná jednomu metru. Na obrázku je tedy vidět zaznamenané monitorování týkající se jednoho přístupového bodu. Střed modrého kruhu určuje místo ve kterém byl naměřen nejlepší signál – protože toto měření probíhalo ve velice husté zástavbě tak jde s největší pravděpodobností o místo, ze kterého byl na přístupový bod přímí výhled a jak je vidět z obrázku č. 32 tak ten přístupový bod byl i velmi blízko – z obrázku odhadem do 5 metrů. Na obrázku č. 33 můžete vidět jak spočítal pozici přístupového bodu nástroj „gps_wi-fi“.



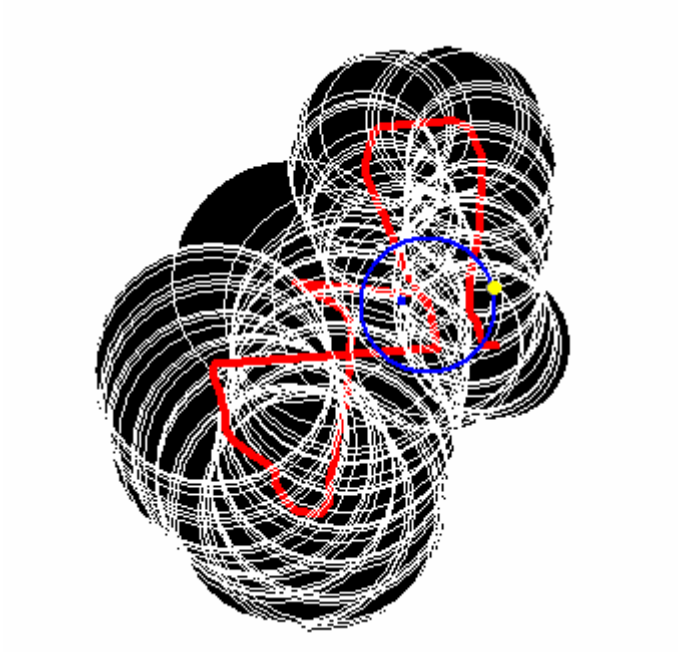
Obrázek č. 33 – naměřená data v nástroji *GPS_WI-FI*

Modrý bod znázorňuje vypočtenou pozici přístupového bodu. V tomto případě byla poloha přístupových bodů počítána ze všech naměřených míst. Zkoušel jsem ještě jiný postup – a to takový, že jsem vycházel z pozice ve které byl naměřen nejlepší signál – modrý kruh na obrázku č. 32 – pozici přístupového bodu jsem počítal pouze z míst které byly do určité experimentální vzdálenosti od tohoto místa s nejlepším signálem – a výsledek je znázorněn na obrázku č. 34. Výpočet v prostoru potom probíhal stejně jako v předešlém případě.



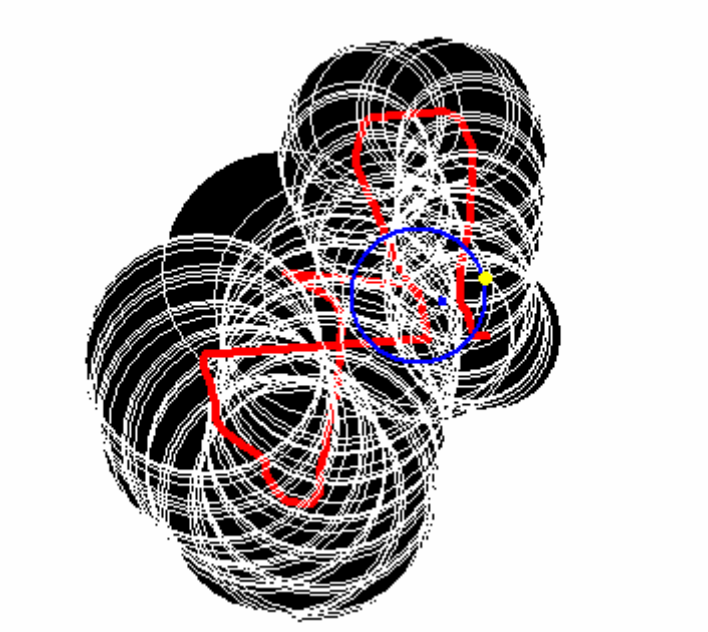
Obrázek č. 34 – naměřená data v nástroji *GPS_WI-FI*

V případě tohoto přístupového bodu se vypočtená pozice přístupového bodu pouze nepatrně přiblížila k místu s nejlepším signálem. Pozice přístupového bodu se počítala z míst měření, které jsou vzdálené od místa s nejlepším signálem maximálně 40 metrů. To, že je pozice přístupového bodu u obou metod výpočtů téměř stejná je v tomto případě způsobeno velkou koncentrací naměřených pozic v oblasti místa s nejlepším signálem. Další příklad je na dalších dvou obrázcích – obrázek č. 35 a obrázek č. 36.



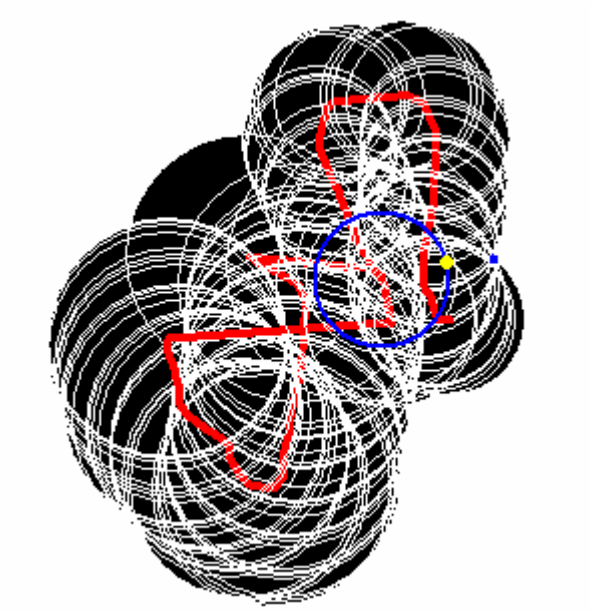
Obrázek č. 35 – naměřená data v nástroji *GPS_WI-FI*

Obrázek č. 35 zobrazuje další měření přístupového bodu – modrý bod zobrazuje vypočítanou pozici přístupového bodu a žlutá tečka značí skutečnou polohu přístupového bodu. Střed modrého kruhu zase značí místo nejlepšího signálu. Na obrázku č. 35 se počítá poloha přístupového bodu ze všech naměřených míst.



Obrázek č. 36 – naměřená data v nástroji *GPS_WI-FI*

Význam jednotlivých barevných bodů na obrázku č. 36 je stejný jako na obrázku č. 35. Pozice přístupového bodu na obrázku č. 36 je počítána pouze z míst, která jsou vzdálená maximálně 40 metrů od místa s nejlepším naměřeným signálem. Pokud nastavím tuto vzdálenost například na 60 až 80 metrů od místa s nejlepším signálem, vypadá výpočet polohy přístupového bodu následovně – obrázek č. 37.



Obrázek č. 37 – naměřená data v nástroji *GPS_WI-FI*

Jak je vidět z obrázků a z výpočtů pozic jednotlivými metodami, tak přesný výpočet polohy přístupového bodu z úrovně wi-fi signálu v měřených místech je prakticky nemožné. Takovéto výpočty v takto hustých zástavbách(sídliště – 12. patrové domy) mají přesnost určení polohy přístupového bodu zhruba +-50 metrů. Proto do databáze ukládám i pozice místa ve kterém byl naměřen nejlepší signál k danému přístupovému bodu – z praktického hlediska to bude určitě stejně užitečné jako přesná pozice přístupového bodu.

6.4 Algoritmy přepočtu souřadných systémů

Zde uvedu algoritmy přepočtu souřadných systému SJTSK a WGS-84 v obou směrech. Algoritmy jsem převzal z internetu – viz literatura, a přepsal je do prostředí nástroje BORLAND DELPHI.

6.4.1 Převod SJTSK na WGS-84

```
function SJTSKTOWGS84(x:real;y:real;h:real):PointWGS84;
var poziceAP:PointWGS84;
    a,e,n,konst_u_ro,sinUQ,cosUQ,sinVQ,cosVQ,alfa,k,ro,epsilon,D,S:real;
    sinS,cosS,sinU,cosU,sinDV,cosDV,sinV,cosV,Ljtsk,t,pom,Bjtsk,sinB:real;
    f_1,e2,x1,y1,z1,dx,dy,dz,wx,wy,wz,m,xn,yn,zn,a_b,p,theta,st,ct:real;
begin
 {h := h + 45; - já pracuji s elipsoidickou výškou = nadmořská + 45m}

{Vypočet zeměpisných souřadnic z rovinných souřadnic}
 e := 0.081696831215303;
 n := 0.97992470462083; konst_u_ro := 12310230.12797036;
 sinUQ := 0.863499969506341; cosUQ := 0.504348889819882;
 sinVQ := 0.420215144586493; cosVQ := 0.907424504992097;
 alfa := 1.000597498371542; k := 1.003419163966575;
```

```
 ro := sqrt(sqr(x) + sqr(y));
 epsilon := 2 * arctan(y / (ro + x));
 D := epsilon / n;
 S := 2 * arctan(exp(1 / n * ln(konst_u_ro / ro))) - PI/2;
 sinS := sin(S);cosS := cos(S);
 sinU := sinUQ * sinS - cosUQ * cosS * cos(D);
 cosU := sqrt(1 - sqr(sinU));
 sinDV := sin(D) * cosS / cosU; cosDV := sqrt(1 - sqr(sinDV));
 sinV := sinVQ * cosDV - cosVQ * sinDV; cosV := cosVQ * cosDV + sinVQ * sinDV;
 Ljtsk := 2 * arctan(sinV / (1 + cosV)) / alfa;
 t := exp(2 / alfa * ln((1 + sinU) / cosU / k));
 pom := (t - 1) / (t + 1);
 repeat
  sinB := pom;
  pom := t * exp(e * ln((1 + e * sinB) / (1 - e * sinB)));
  pom := (pom - 1) / (pom + 1);
 until (abs(pom - sinB) <= 1e-15);
 Bjtsk := arctan(pom / sqrt(1 - sqr(pom)));

{ Pravoúhlé souřadnice ve S-JTSK }

  a := 6377397.15508; f_1 := 299.152812853;
  e2 := 1 - (1 - 1 / f_1) * (1 - 1 / f_1);
  ro := a / sqrt(1 - e2 * sin(Bjtsk) * sin(Bjtsk));
  x1 := (ro + h) * cos(Bjtsk) * cos(Ljtsk);
  y1 := (ro + h) * cos(Bjtsk) * sin(Ljtsk);
  z1 := ((1 - e2) * ro + h) * sin(Bjtsk);

{ Pravoúhlé souřadnice v WGS-84}

  dx := 570.69; dy := 85.69; dz := 462.84;
  wz := -5.2611 / 3600 * PI / 180;
  wy := -1.58676/3600 * PI/180;
  wx := -4.99821/3600 * PI / 180; m := 3.543e-6;
  xn := dx + (1 + m) * (x1 + wz * y1 - wy * z1);
  yn := dy + (1 + m) * (-wz * x1 + y1 + wx * z1);
  zn := dz + (1 + m) * (wy * x1 - wx * y1 + z1);

{ Geodetické souřadnice v systému WGS-84}

  a := 6378137.0; f_1 := 298.257223563;
  a_b := f_1 / (f_1 - 1); p := sqrt(sqr(xn) + sqr(yn));
  e2 := 1 - (1 - 1 / f_1) * (1 - 1 / f_1);
  theta := arctan(zn * a_b / p); st := sin(theta); ct := cos(theta);
  t := (zn + e2 * a_b * a * st * st * st) / (p - e2 * a * ct * ct * ct);
  poziceAP.lat := arctan(t);  poziceAP.lon := 2 * arctan(yn / (p + xn));
  poziceAP.height := sqrt(1 + sqr(t)) * (p - a / sqrt(1 + (1 - e2) * sqr(t)));

  poziceAP.lat := poziceAP.lat /PI*180;
  poziceAP.lon := poziceAP.lon /PI*180;

  SJTSKTOWGS84 := poziceAP;
end;
```

Vstupními proměnnými této funkce jsou proměnné *x,y* a *h*. Výstupem této funkce je struktura obsahující zeměpisnou šířku, délku a výšku v podobě tří reálných čísel. [29]

6.4.2 Převod WGS-84 na SJTSK

```
function WGSTOSJTSK(sirka,delka,vyska:string):POINTOFSJTSK;
var sirkaprevod,delkaprevod,vyskaprevod,a,f_1,e2,ro,x,y,z:real;
       wx,wy,wz,dx,dy,dz,m,xn,yn,zn,p,a_b,theta,st,ct,t,n,konst_u_ro:real;
       sinUQ,sinVQ,cosUQ,cosVQ,alfa,k_2,sinB,e,sinU,cosU,V,cosV,sinV:real;
       sinDV,cosDV,sinS,cosS,sinD,D,epsilon,X1,Y1:real;
       RC:real;
       BODSJTSK : POINTOFSJTSK
begin
RC := 3.14159265358979323846264338327 95;
sirkaprevod := StrtoFloat(sirka);
delkaprevod := StrtoFloat(delka);
vyskaprevod := StrtoFloat(vyska);
sirkaprevod := sirkaprevod/180*RC;
delkaprevod := delkaprevod/180*RC;
```

```
a:=6378137.0; f_1:=298.257223563;
e2:=1-(1-1/f_1)*(1-1/f_1);ro:=a/sqrt(1-e2*sin(sirkaprevod)*sin(sirkaprevod));
x:=(ro+vyskaprevod)*cos(sirkaprevod)*cos(delkaprevod);
y:=(ro+vyskaprevod)*cos(sirkaprevod)*sin(delkaprevod);
z:=((1-e2)*ro+vyskaprevod)*sin(sirkaprevod);
dx:=-570.69;dy:=-85.69;dz:=-462.84;
wz:=5.2611/3600*RC/180;
wy:=1.58676/3600*RC/180;
wx:=4.99821/3600*RC/180; m:=-3.543e-6;
xn:=dx+(1+m)*(x+wz*y-wy*z);yn:=dy+(1+m)*(-wz*x+y+wx*z);zn:=dz+(1+m)*(wy*x-wx*y+z);
a:=6377397.15508;f_1:=299.152812853;
a_b:=f_1/(f_1-1);p:=sqrt(xn*xn+yn*yn);e2:=1-(1-1/f_1)*(1-1/f_1);
theta:=arctan(zn*a_b/p);st:=sin(theta);ct:=cos(theta);
t:=(zn+e2*a_b*a*st*st*st)/(p-e2*a*ct*ct*ct);
sirkaprevod:=arctan(t);delkaprevod:=2*arctan(yn/(p+xn));
vyskaprevod:=sqrt(1+t*t)*(p-a/sqrt(1+(1-e2)*t*t));
a:=6377397.15508;e:=0.081696831215303;
n:=0.97992470462083;konst_u_ro:=12310230.12797036;
sinUQ:=0.863499969506341;cosUQ:=0.504348889819882;
sinVQ:=0.420215144586493;cosVQ:=0.907424504992097;
alfa:=1.000597498371542;k_2:=1.00685001861538;
sinB:=sin(sirkaprevod);t:=(1-e*sinB)/(1+e*sinB);
t:=sqr((1+sinB))/(1-sqr(sinB))*exp(e*ln(t));
t:=k_2*exp(alfa*ln(t));
sinU:=(t-1)/(t+1);cosU:=sqrt(1-sqr(sinU));
V:=alfa*delkaprevod;sinV:=sin(V);cosV:=cos(V);
cosDV:=cosVQ*cosV+sinVQ*sinV;sinDV:=sinVQ*cosV-cosVQ*sinV;
sinS:=sinUQ*sinU+cosUQ*cosU*cosDV;cosS:=sqrt(1-sqr(sinS));
sinD:=sinDV*cosU/cosS;D:=arctan(sinD/sqrt(1-sqr(sinD)));
epsilon:=n*D;ro:=konst_u_ro*exp(-n*ln((1+sinS)/cosS));
X1:=ro*cos(epsilon);Y1:=ro*sin(epsilon);
BODSJTSK.x := X1; BODSJTSK.y := Y1; BODSJTSK.z := vyskaprevod;

WGSTOSJTSK := BODSJTSK;
end;
```

Vstupní proměnné této funkce tvoří zeměpisné souřadnice WGS-84 v podobě reálných čísel, ale typu string – reálné číslo zapsané jako řetězec. Výstupem je záznam obsahující tři reálná čísla představující souřadnice *x,y* a *z* v souřadném systému SJTSK. [28]

6.5 Databáze

Jak je vidět z obrázku č. 18, tak databáze je poměrně jednoduchá. Jednotlivé tabulky jsou mezi sebou svázané přes své *id*, které tvoří zároveň primární klíče – jsou červeně podtržené. Význam jednotlivých názvů sloupců v tabulkách zde nebudu vysvětlovat – pouze ty u kterých není z názvu přímo jasné jaký mají význam nebo jakých hodnot nabývají. Sloupec s označením „stav“ u jednotlivých tabulek nabývá hodnot 1,2 nebo 3 – 1 = záznam existuje, 2 = záznam již neexistuje, 3 = záznam byl vložen do databáze omylem. Sloupec „typ“ v tabulce Mcast nabývá hodnot - 1 = městská část , 2 = městský obvod, 3 = nečleněná část obce. Sloupec „typcdomu“ v tabulce Objekt nabývá hodnot - 1 = číslo popisné, 2 = číslo evidenční.

Sloupce tabulky s názvem *Wifi_Pristupove_Body* popíši raději všechny, protože jejich význam nemusí být z názvu zcela jednoznačný. *BSSID* – představuje mac adresu přístupového bodu, *SSID* – název přístupového bodu, *VENDOR* – popis přístupového bodu – výrobce, *ENCRYPT* – ano nebo ne – jestli je komunikace s přístupovým bodem šifrovaná, *DATE* – datum kdy proběhlo změření přístupového bodu, *CHANNEL* – kanál na kterém pracuje přístupový bod, *MODE* – topologie sítě přístupového bodu, *RATES* – představuje seznam podporovaných rychlostí přístupového bodu, *LATSPWGS* + *LONGAPWGS* + *HEIAPWGS* – představují zeměpisné souřadnice polohy přístupového bodu v souřadném systému WGS-84, *CHYBA* – součet rozdílů vzdáleností při výpočtu pozice přístupového bodu,*XAPSJTSK* + *YAPSJTSK* + *ZAPSJTSK* – pozice přístupového bodu v souřadném systému SJTSK, *PCHYBA* – průměr ze součtů vzdáleností, *LATBESTSIGWGS* + *LONBESTSIGWGS* + *HEIBESTSIGWGS* – poloha místa s nejlepším naměřeným signálem

souřadném systému WGS-84, *XBESTSIGSJTSK* + *YBESTSIGSJTSK* + *ZBESTSIGSJTSK* - poloha místa s nejlepším naměřeným signálem v souřadném systému SJTSK, *DISBESTSIG* – vzdálenost místa s nejlepším naměřeným signálem od polohy přístupového bodu – od skutečné polohy přístupového bodu.

Data jsem do databáze nahrál pomocí vytvořeného php skriptu. Data se do databáze nahrávají ze souborů typu .csv. Strukturu a obsah jednoho takového souboru můžete vidět na následujícím výpisu.

Výpis ze zdrojového souboru *Kraje* :

```
19,'CZ011',19,'Hlavní město Praha','Hl. m. Praha',1,'2000-01-01',,,
27,'CZ021',27,'Středočeský','Středočeský',1,'2000-01-01',,,
35,'CZ031',35,'Jihočeský','Jihočeský',1,'2000-01-01',,,
43,'CZ032',35,'Plzeňský','Plzeňský',1,'2000-01-01',,,
51,'CZ041',43,'Karlovarský','Karlovarský',1,'2000-01-01',,,
60,'CZ042',43,'Ústecký','Ústecký',1,'2000-01-01',,,
78,'CZ051',51,'Liberecký','Liberecký',1,'2000-01-01',,,
86,'CZ052',51,'Královéhradecký','Královéhradecký',1,'2000-01-01',,,
94,'CZ053',51,'Pardubický','Pardubický',1,'2000-01-01',,,
108,'CZ061',60,'Vysočina','Vysočina',1,'2000-01-01',,,
116,'CZ062',60,'Jihomoravský','Jihomoravský',1,'2000-01-01',,,
124,'CZ071',78,'Olomoucký','Olomoucký',1,'2000-01-01',,,
132,'CZ081',86,'Moravskoslezský','Moravskoslezský',1,'2000-01-01',,,
141,'CZ072',78,'Zlínský','Zlínský',1,'2000-01-01',,,
```

Na předchozím výpisu je vidět obsah a struktura souboru pro naplnění tabulky Kraje. Jednotlivé hodnoty budoucích sloupců tabulky Kraje jsou oddělené čárkou. Pořadí jednotlivých hodnot je podrobně popsáno v dokumentaci územně identifikačního registru adres – proto nemá smysl je zde vypisovat. Jak je vidět tak soubory obsahují daleko více informací než využívám ve své databázi – některé z nich nejsou povinné – proto jsou u některých řádků například tři čárky za sebou. Ve své databázi používám vesměs data, která jsou v územně identifikačním registru adres povinná. Ostatní soubory pro naplnění mé databáze mají stejnou strukturu – je zbytečné ukazovat zde příklady všech.

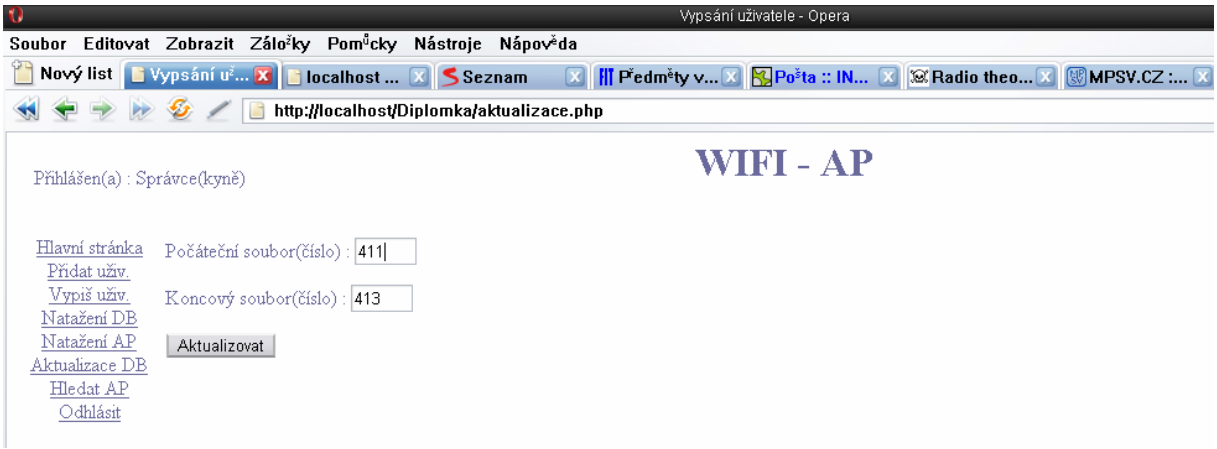
Podobně to vypadá i se soubory pro aktualizaci této databáze. Obsah a struktura části souboru pro aktualizaci je vidět v následujícím výpisu.

Výpis z aktualizačního souboru :

```
0;UIR-ADR;4;4;2;411;03/04;13.05.2004-14:57:29
7;1;K_3203/226;1=734519;2=533025;3=Buková;4=Buková;5=1;6=02.01.2004
7;1;K_3203/226;1=734535;2=533025;3=Jílová;4=Jílová;5=1;6=02.01.2004
55;1;K_3505/63;1=105959;2=556904;3=408956;4=254193;5=46005
55;1;K_3505/63;1=105960;2=556904;3=408883;5=46001
55;1;K_3505/63;1=105961;2=556904;3=408760;4=257087;5=46001
55;1;K_3505/63;1=105962;2=556904;3=408832;4=258814;5=46001
999;05026
```

Aktualizační soubor je textový soubor s délkou řádku max. 2000 znaků (včetně ukončujících znaků *CR* a *LF*). Každý řádek tohoto souboru tvoří jeden příkaz. Příkaz je tvořen posloupností parametrů. Parametry v příkazu jsou navzájem odděleny znakem středník. Za posledním parametrem v příkazu tento oddělovač není. Parametr je buď řídící údaj změnového souboru nebo výraz tvaru kód atributu = hodnota atributu pro nějaký atribut záznamu tabulky databáze UIR-ADR. První řádek tvoří příkaz záhlaví a poslední příkaz tvoří

příkaz konce. Mezi prvním a posledním řádkem jsou změnové příkazy. První a poslední řádek pro mě není důležitý – proto je nebudu popisovat. Důležité jsou změnové příkazy jejichž strukturu popíši – změnový příkaz = kód tabulky; kód operace; dokument; kód atributu = hodnota atributu ; . . . ; kód atributu = hodnota atributu *CRLF*. **Kód tabulky** = číselný kód tabulky databáze UIR-ADR, jíž se změnová operace týká. Kód tabulky je celé číslo bez znaménka, bez úvodních nul a bez mezer. **Kód operace** = číselný kód změnové operace: 0 = *DELETE*, 1 = *INSERT*, 2 = *UPDATE*. **Dokument** = označení dokumentu o změně, na jehož základě byla změna provedena. **Kód atributu** = číselný kód atributu, jehož hodnota je uvedena za rovnítkem. Kód atributu je celé číslo bez znaménka, bez úvodních nul a bez mezer. **Hodnota atributu** = hodnota atributu. Každý aktualizační soubor je očíslován – pěti místné číslo, které je zleva doplněno nulami tak aby mělo pět míst. Databáze, kterou jsem získal měla verzi dat číslo 00410. Na webu Ministerstva práce a sociálních věcí [27] byly k dispozici aktualizační soubory číslo *00411* až *00577*. Aktualizaci jsem naimplementoval tak, že stačí zadat počáteční a koncové číslo souboru a proběhne aktualizace všech souborů od počátečního do koncového čísla.Aktualizace je znázorněna na obrázku č. 38.

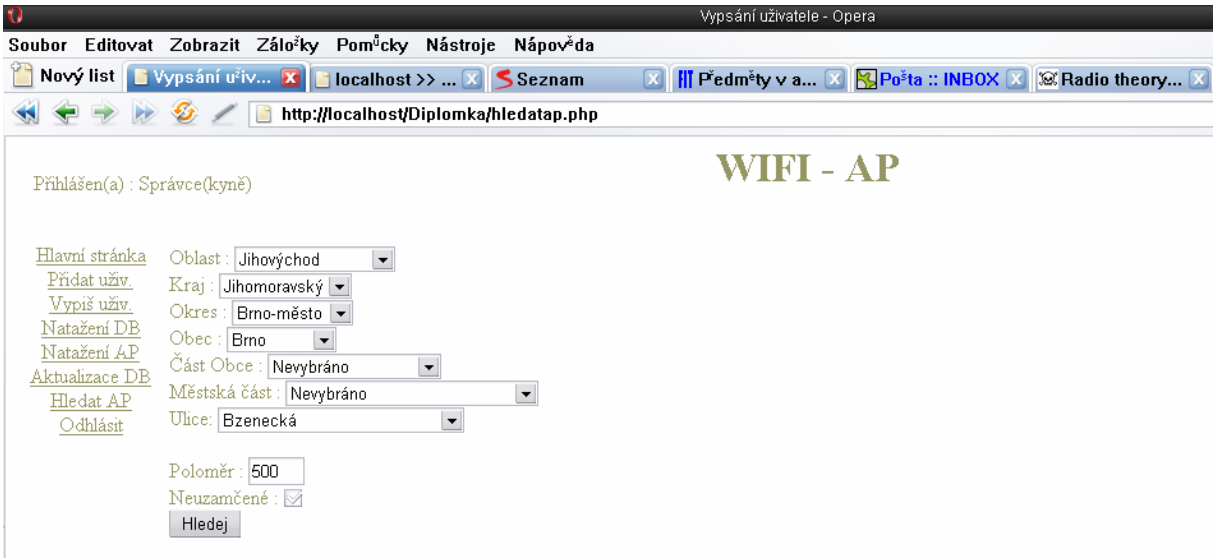


Obrázek č. 38 – webové rozhraní

Počáteční natažení dat proběhne pouze jednou na počátku – rozhraní jak jsem jej naimplementoval je znázorněno na obrázku č. 39.

Obrázek č. 39 – webové rozhraní

Vyhledávání přístupových bodů potom probíhá tak, že si uživatel vybere oblast, kraj, okres, obec a dále už si jenom zvolí část obce nebo městskou část nebo ulici. Nejlepší je zvolit ulici pokud je to možné, protože ta je přímo napojena na tabulku Adresa. Při vyhledávání se potom spočítá průměrná poloha všech adres z vámi vybrané oblasti a najde v databázi všechny přístupové body jejichž vzdálenost od průměrné polohy všech adres je menší nebo rovna vámi zadanému poloměru v metrech. Vyhledávání je znázorněno na obrázku č. 40.



Obrázek č. 40 – webové rozhraní

Webové rozhraní jsem navrhl pro uživatele dvou druhů – první z nich je správce, který může ovládat a dělat naprosto vše – ovládat databázi, spravovat uživatele a vyhledávat přístupové body, druhý je normální uživatel, který může pouze vyhledávat přístupové body.

7. Závěr

Ze získaných výsledků, měření(monitorování) a výpočtů pozic přístupových bodů je patrné, že výpočet vzdálenosti od přístupového bodu podle síly signálu v daném místě a následný výpočet pozice přístupového bodu je velmi nepřesný a řekl bych, že v takto hustě zastavěné oblasti, ve které jsem monitorování prováděl, je i nemožný. Vypočítaná poloha přístupového bodu se lišila od skutečné polohy v průměru zhruba o vzdálenost 50 metrů – v některých špatně naměřených případech to bylo i horší. Na druhou stranu je do databáze ukládána i pozice nejlepšího naměřeného signálu, u které se pohybovala vzdálenost k přístupovému bodu v průměru kolem 30 metrů – samozřejmě to záleží na oblasti ve které monitorování provádíte a také jakým způsobem monitorování provádíte. Nepřesnost výpočtu je způsobena jednak mírou zastavění(budovami) v dané oblasti, ale hlavně také nepřesnou informací o velikosti signálu, kterou udává program „netstumbler" – což je vidět i z obrázků – v různých vzdálenostech od přístupového bodu je intenzita signálu například stejná a to i v rozmezí 100 metrů – takže potom z takových dat určit přesnou pozici přístupového bodu je nemožné.

Možnosti dalšího rozšíření projektu :

Rozšíření tohoto projektu vidím ve spojení s mapovými systémy a následném zobrazování získaných dat o přístupových bodech do mapových podkladů. Také by bylo možné provádět různé statistické průzkumy v oblasti pokrytí a počtu přístupových bodů v dané oblasti.

8. Literatura

[1] Ladislav Bittner , Jak se neztratit aneb vše podstatné o GPS, Dostupný z WWW: <http://www.novinky.cz/archiv/Index/Pocitace_a_technika/9829.html >, 23. 9. 2003
[2] Wikipedia, Global Positioning system, Dostupný z WWW: < http://cs.wikipedia.org/wiki/Global_Positioning_System > ,
[3] Štěpán Vávra, Trendy ve zpracování a používání sítí WLAN, Dostupný z WWW: < http://access.feld.cvut.cz/rservice.php?akce=tisk&cisloclanku=2005112301 > , 20.1. 2006
[4] wifionline.net, Bezdrátové sítě LAN a bezpečnost dle WIFI, Dostupný z WWW: < http://mikrovlny.cz/wifibezpecnost.html >
[5] Wikipedia, WIFI, Dostupný z WWW: < http://cs.wikipedia.org/wiki/Wi-Fi >
[6] Slovníček pojmů, Dostupný z WWW: < http://802.11b.cz/pojmy.asp >
[7] Jaroslav Snášel, Už vím, jak pracuje navigační systém GPS, Dostupný z WWW: < http://www.mobilmania.cz/default.aspx?article=1111127 >, 21.10. 2005
[8] Jaroslav Snášel, Už vím, jak pracuje navigační systém GPS, Dostupný z WWW: < http://www.mobilmania.cz/default.aspx?section=21&server=1&article=1111127&chapter=1030454 > , 21.10. 2005
[9] Jan Martinek, GPS a komunikační protokol NMEA, Dostupný z WWW: < http://www.abclinuxu.cz/clanky/ruzne/gps-a-komunikacni-protokol-nmea-1-princip-historie >, 6.9. 2006
[10] Jak zabezpečit bezdrátovou síť , Dostupný z WWW: < http://www.xmaestro.com/view.php?nazevclanku=jak-zabezpecit-bezdratovou-sit&cisloclanku=2006100024 >, 8.10. 2006
[11] WIFI sítě a jejich slabiny, Dostupný z WWW: < http://www.security-portal.cz/clanky/wifi-site-a-jejich-slabiny.html >
[12] Microsoft, Je vaše domácí bezdrátová síť ohrožena?, Dostupný z WWW: < http://www.microsoft.com/cze/athome/security/online/homewireless.mspx >, 22.4. 2005
[13] Warchalking, Dostupný z WWW: < http://www.security-portal.cz/clanky/warchalking.html >
[14] Jan Martinek, GPS a komunikační protokol NMEA 2, Dostupný z WWW: < http://www.abclinuxu.cz/clanky/ruzne/gps-a-komunikacni-protokol-nmea-2-dostupnost-presnost-navilock >, 26.9. 2006
[15] Jan Martinek, GPS a komunikační protokol NMEA 3, Dostupný z WWW: < http://www.abclinuxu.cz/clanky/ruzne/gps-a-komunikacni-protokol-nmea-3-dekodovani-dat >, 10.10. 2006
[16] Rita Pužmanová, Bezdrátové lokální sítě WLAN podle ieee 2, Dostupný z WWW: < http://www.lupa.cz/clanky/bezdratove-lokalni-site-wlan-podle-ieee-ii/ >, 16.4. 2002
[17] Daniel Dočkal, Warchalking a WIFI sítě vůbec, Dostupný z WWW: < http://www.pooh.cz/clanky/warchalking/warchalking.asp>
[18] Ovanet, Dostupný z WWW: < http://www.ovanet.cz/files/Wi-Fi%20FAQ.pdf > , 26.12. 2004
[19] Dostupný z WWW: < http://www.freedownloadscenter.com/Best/wifi-api-delphi.html >
[20] Petr Lasek, Bezdrátové sítě – standard 802.11, Dostupný z WWW: < http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=115&clanekID=123 >, 23.7. 2001
[21] Lee Barken, Kniha - Jak zabezpečit bezdrátovou síť WIFI – Computer Press 2004
[22] Thomas Kohre, Kniha - Stavíme si bezdrátovou síť WIFI – Computer Press 2004
[23] Patrick Zandl, Kniha - Bezdrátové sítě WIFI – Praktický průvodce – Computer Press 2003
[24] Nástroj netstumbler, Dostupný z WWW: < http://www.netstumbler.com >
[25] Nástroj cain, Dostupný z WWW: < http://www.oxid.it >
[26] axgps, komponenta gps pro Delphi, Dostupný z WWW: < http://www.shareit.com/105283-1.html >
[27] UIR-ADR, databáze územně identifikačního registru adres , Dostupný z WWW: < http://forms.mpsv.cz/uir/default2.jsp >
[28] Zdeněk Hrdina, přepočet souřadnic z WGS-84 do SJTSK, Dostupný z WWW: < http://www.gpsweb.cz/WGStoJTSK.html >, 2001
[29] Zdeněk Hrdina, přepočet souřadnic z WGS-84 do SJTSK , Dostupný z WWW: < http://www.gpsweb.cz/JTSK-WGS.htm >, 2002
[30] Mathias Coinchon, wi-fi výpočty, Dostupný z WWW: < http://www.swisswireless.org/wlan_calc_en.html >, 13.1. 2003
[31] CzFree.net, wi-fi výpočty, Dostupný z WWW: < https://twiki.klfree.net/twiki/bin/view/SpravaSite/NastaveniVykonuXi626 >

9. Seznam příloh

Příloha 1. Manuál ...
Příloha 2. CD ...